10/507212
DT04 Rec'd PCT/PTO 15 SEP 2004

DOCKET NO.: 257756US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Miki MURAKAMI, et al.
SERIAL NO.: NEW U.S. PCT APPLICATION
FILED: HEREWITH
INTERNATIONAL APPLICATION NO.: PCT/JP03/16623
INTERNATIONAL FILING DATE: December 24, 2003
FOR: CONTENTS DISTRIBUTION SYSTEM, INFORMATION PROCESSING APPARATUS OR METHOD, AND COMPUTER PROGRAM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-014245	23 January 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/16623. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

PCT/JP03/16623
Rec'd PCT/PTO 15 SEP 2004
24.12.03
10/507212

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

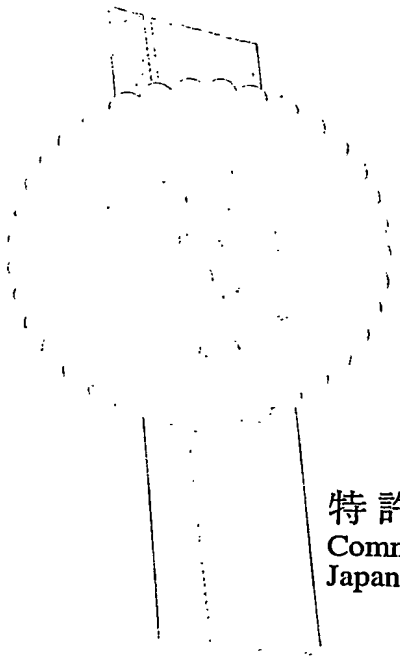
出願年月日
Date of Application: ２００３年　１月２３日

REC'D 19 FEB 2004
WIPO PCT

出願番号
Application Number: 特願２００３－０１４２４５

[ST. 10/C]: [ＪＰ２００３－０１４２４５]

出願人
Applicant(s): ソニー株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　２月　５日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３００６５６０

【書類名】　特許願
【整理番号】　0290853204
【提出日】　平成15年 1月23日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　村上　幹
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　久松　史明
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100093241
　【弁理士】
　【氏名又は名称】　宮田　正昭
【選任した代理人】
　【識別番号】　100101801
　【弁理士】
　【氏名又は名称】　山田　英治
【選任した代理人】
　【識別番号】　100086531
　【弁理士】
　【氏名又は名称】　澤田　俊夫

【手数料の表示】

【予納台帳番号】　048747

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ配信システム、情報処理装置又は情報処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

ユーザのクライアントにコンテンツを配信するコンテンツ配信システムであって、ユーザは２以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

ユーザの各クライアントを登録して顧客関連情報を取得する登録手段と、

顧客関連情報を管理する顧客関連情報管理手段と、

クライアントからの要求に応じて該要求元クライアントへコンテンツを提供するコンテンツ提供手段と、

前記コンテンツ提供手段からコンテンツを取得したクライアントからの要求に応じて該要求元クライアントへ該取得コンテンツについてのライセンスを提供するライセンス提供手段と、

同一ユーザが持つ１つのクライアントから他のクライアントへのコンテンツの移動が正当であることを示すコンテンツ・コピー証明書を該移動元のクライアントに提供するコンテンツ・コピー証明書提供手段と、

を具備することを特徴とするコンテンツ配信システム。

【請求項２】

前記コンテンツ・コピー証明書提供手段は、移動先のクライアントに対するライセンスを含んだコンテンツ・コピー証明書を生成する、

ことを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項３】

コンテンツ移動元及びコンテンツ移動先の各クライアントはそれぞれ異なるライセンス提供手段に登録され、各ライセンス提供手段は登録クライアントに対して自己の公開鍵を提供し、

前記コンテンツ・コピー証明書提供手段は、コンテンツ移動先のクライアントが登録されているライセンス提供手段の秘密鍵を用いてコンテンツ・コピー証明

書に電子署名を施す、

ことを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項４】

前記コンテンツ・コピー証明書提供手段は、

前記コンテンツ移動元のクライアントから移動対象となるコンテンツについてのライセンスＩＤと移動先のクライアントのクライアントＩＤを取得し、

前記顧客関連情報関連手段に照会して、移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを確認してからコンテンツ・コピー証明書を提供する、

ことを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項５】

前記顧客関連情報管理手段は、リーフＩＤとクライアントＩＤの対応テーブル、クライアントＩＤとクライアントの公開鍵証明書の対応テーブル、クライアントＩＤとユーザＩＤの対応テーブル、コンテンツＩＤとライセンスＩＤの対応テーブル、ユーザＩＤとダウンロードしたコンテンツのコンテンツＩＤの対応テーブル、ユーザＩＤとダウンロードしたライセンスのライセンスＩＤの対応テーブル、コンテンツ・コピー証明書の発行履歴を管理する、

ことを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項６】

前記顧客関連情報管理手段は、前記コンテンツ提供手段がクライアントにコンテンツを提供し、及び／又は、前記ライセンス提供手段がクライアントにライセンスを提供する度に顧客関連情報を更新する、

ことを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項７】

クライアントへのライセンス提供及び／又はコンテンツ・コピー証明書の提供に応じてクライアントへの課金処理を行なう課金処理手段をさらに備える、

ことを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項８】

前記課金処理手段は、ライセンスを提供する場合とコンテンツ・コピー証明書を提供する場合とで差額を設ける、
ことを特徴とする請求項５に記載のコンテンツ配信システム。

【請求項９】

コンテンツを使用する情報処理装置であって、

コンテンツをダウンロードするコンテンツ・ダウンロード手段と、

コンテンツを蓄積するコンテンツ蓄積手段と、

コンテンツを利用するためのライセンスを取得するライセンス取得手段と、

取得したライセンスを用いてコンテンツを正当に利用するコンテンツ再生手段と、

コンテンツ移動のためのコンテンツ・コピー証明書を取得するコンテンツ・コピー証明書取得手段と、

前記コンテンツ蓄積手段に蓄積されたコンテンツにコンテンツ・コピー証明書を付加して同一ユーザが所持する他の機器に移動し、又は、コンテンツ・コピー証明書が付加されたコンテンツを同一ユーザが所持する他の機器から取得し、該コンテンツ・コピー証明書の正当性を検証しライセンスを取り出すとともにコンテンツを前記コンテンツ蓄積手段に格納するコンテンツ移動手段と、
を具備することを特徴とする情報処理装置。

【請求項１０】

前記情報処理装置はライセンス・サーバに登録してその公開鍵を受け取り、

コンテンツ・コピー証明書はライセンス・サーバの秘密鍵で電子署名が施されており、

前記コンテンツ移動手段は、外部から取得したコンテンツ・データに付加されているコンテンツ・コピー証明書の改竄の有無を前記ライセンス・サーバの公開鍵を用いてチェックする、
ことを特徴とする請求項９に記載の情報処理装置。

【請求項１１】

コンテンツを使用する情報処理方法であって、

コンテンツをダウンロードするコンテンツ・ダウンロード・ステップと、

コンテンツを蓄積するコンテンツ蓄積ステップと、

コンテンツを利用するためのライセンスを取得するライセンス取得ステップと、

取得したライセンスを用いてコンテンツを正当に利用するコンテンツ再生ステップと、

コンテンツ移動のためのコンテンツ・コピー証明書を取得するコンテンツ・コピー証明書取得ステップと、

前記コンテンツ蓄積ステップにおいて蓄積されたコンテンツにコンテンツ・コピー証明書を付加して同一ユーザが所持する他の機器に移動し、又は、コンテンツ・コピー証明書が付加されたコンテンツを同一ユーザが所持する他の機器から取得し、該コンテンツ・コピー証明書の正当性を検証しライセンスを取り出すとともにコンテンツを格納するコンテンツ移動ステップと、

を具備することを特徴とする情報処理方法。

【請求項１２】

ライセンス・サーバに登録してその公開鍵を受け取るステップをさらに備え、

コンテンツ・コピー証明書はライセンス・サーバの秘密鍵で電子署名が施されており、

前記コンテンツ移動ステップでは、外部から取得したコンテンツ・データに付加されているコンテンツ・コピー証明書の改竄の有無を前記ライセンス・サーバの公開鍵を用いてチェックする、

ことを特徴とする請求項１１に記載の情報処理方法。

【請求項１３】

コンテンツを使用するためのライセンスを提供する処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、ユーザは２以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

コンテンツ移動元のクライアントから移動対象となるコンテンツについてのライセンスＩＤとコンテンツ移動先のクライアントのクライアントＩＤを取得するステップと、

コンテンツ移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを判別するステップと、

コンテンツ・コピー証明書を作成するステップと、

コンテンツ・コピー証明書をコンテンツ移動元のクライアントに提供するステップと、

を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークなどによって配信される音楽データや画像データ、電子出版物などのデジタル・データや動画像などのコンテンツの利用を管理するコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに係り、特に、使用許諾など何らかの契約や利用条件に基づいてコンテンツの利用を管理するコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに関する。

【０００２】

さらに詳しくは、本発明は、コンテンツの利用者にライセンスを与えることによりコンテンツの利用を制御しコンテンツの保護を図るコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに係り、特に、コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にするコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに関する。

【０００３】

【従来の技術】

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各

種のデジタル・コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網（ｘＤＳＬ：x Digital Subscriber Line、CATV (Cable TV)、無線ネットワークなど）の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組みが整いつつある。

【０００４】

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起こっている。

【０００５】

暗号技術を用いることによって、通信路上に流れるコンテンツを悪意のある第三者から保護することが可能となっている。しかしながら、コンテンツの配信過程だけでなく、コンテンツが正規のユーザに提供された後に行なわれる不正コピーや不正利用も大きな問題となっている。

【０００６】

デジタル･コンテンツに関するこの種の問題への対策として、最近では権利管理方式（ＤＲＭ：Digital Rights Management）と呼ばれる方式が採用されている。以下では、このＤＲＭの概要とその問題点について説明する。

【０００７】

ＤＲＭ（Digital Right Management）：

権利情報管理方式（ＤＲＭ）によって、ユーザはコンテンツの利用許可（ライセンス）を得なければ，コンテンツを利用できない仕組みが実現される。このようなシステムとしては米マイクロソフト社の"Windows Media Right Manager"や、米ＩＢＭ社の"Electronic Media Management System（ＥＭＭＳ）"と呼ばれるシステムが挙げられる。

【０００８】

ＤＲＭのシステムは、典型的にはコンテンツ提供者とライセンス管理者とユーザという参加者で構成される。ユーザは、コンテンツの再生装置を所持し、それを使ってコンテンツを利用する。また、ライセンス管理者は、ユーザにライセンスの発行を行なう。また、コンテンツ提供者は、ユーザにコンテンツの提供を行なう。

【０００９】

コンテンツ（Ｃｏｎｔ）は、コンテンツ提供者によって、コンテンツ毎に異なる鍵（コンテンツ鍵K_c）で暗号化された形式Ｅ（K_c，Ｃｏｎｔ）で配布される。本明細書中では、これを「暗号化コンテンツ」と呼ぶことにする。

【００１０】

ユーザは、あるコンテンツＣｏｎｔを使用する場合、ライセンス管理者に対してライセンス発行を要求する。これに対し、ライセンス発行者は、ユーザへの課金処理などを行なった上でライセンスを発行する。

【００１１】

ここで言うライセンスの発行は、実際には、ユーザの再生装置にコンテンツ鍵K_cを与えることである。このために、ライセンス管理者は再生装置との間で、再生装置毎に異なる暗号鍵K_uを共有しており（暗号鍵K_uの共有は、ライセンス発行時に行なわれるか、又はあらかじめ共有したものが再生装置に組み込まれている）、コンテンツ鍵K_cを暗号鍵K_uで暗号化したデータＥ（K_u，K_c）として再生装置に送付する。このデータのことを「ライセンス・トークン」と呼ぶ。

【００１２】

ライセンスを受けたユーザの再生装置は、暗号鍵K_uと受け取ったライセンス・トークンＥ（K_u，K_c）と暗号化コンテンツＥ（K_c，Ｃｏｎｔ）を使って、コンテンツを再生することができる。まず、ライセンス・トークンＥ（K_u，K_c）からコンテンツ鍵K_cを復号し、次いでコンテンツ鍵Ｋｃを使って暗号化コンテンツＥ（K_c，Ｃｏｎｔ）からコンテンツＣｏｎｔを復号して再生する。したがって、再生装置とライセンス・トークンと暗号化コンテンツの組み合わせが正しいときだけ、つまりライセンスを得たユーザだけがコンテンツを利用でき

ることになる。

【００１３】

ここで、コンテンツの利用権を保護するためには、再生装置側では、復号されたコンテンツが外部に漏洩することを防がなければならない。このためには、再生装置は、暗号鍵Ｋ$_u$やコンテンツ鍵Ｋ$_c$や復号されたコンテンツＣｏｎｔを外部に漏らさないように処理しなければならない。何故なら、復号されたコンテンツが一旦外部に漏洩すれば、それを複製し利用することが制約なしに可能になるからである。言い換えれば、再生装置には、暗号鍵Ｋ$_u$やコンテンツ鍵Ｋ$_c$、並びに復号されたコンテンツＣｏｎｔを外部に漏らさないで処理できるという条件が必要である。本明細書中では、このような条件を備えた再生装置のことを「正当」であると呼ぶことにする。

【００１４】

ＤＲＭでは、コンテンツのライセンス（利用許可）をユーザに与えることは、コンテンツ鍵Ｋ$_c$をそのユーザの（特定の）再生装置に与えることで実現される。このライセンス供与の際に、コンテンツ鍵Ｋ$_c$を受け取る再生装置は正当であるという条件が必須である。したがって、ライセンスの発行を行なうライセンス発行者は、発行相手の再生装置を特定し、正当な再生装置だけにコンテンツ鍵を与えるようにしなければならない。このため、ライセンス発行者は正当な再生装置に関するデータベースを持ち、ライセンス発行はそれに基づいて行なう必要がある。

【００１５】

しかしながら、多数の再生装置が存在する場合を考えると、このようなデータベースの検索は時間あるいはコストを要する処理となる。特に、コンテンツの毎回ダウンロードなどの仕組みにより、ライセンス発行が頻繁に行なわれる場合、データベースの置かれるサーバの負荷が過剰になる。つまり、ＤＲＭでのライセンス発行は、再生装置の個数の増加に対してスケーラビリティのない処理となる。

【００１６】

例えば、特定のユーザに対してコンテンツを提供する場合、コンテンツ提供の

前にユーザ認証を行なうことになる。ＤＲＭの方法を使うのであれば、さらにユーザ認証に加えてそのユーザが持つコンテンツの再生装置を特定し、再生装置毎にライセンスを生成するという処理が必要になる。このことはコンテンツ提供の処理速度を低下させてしまう。

【００１７】

また、ユーザは一般に複数のコンテンツ再生装置を所有し利用するところ、コンテンツのライセンスは特定の再生装置に対して与えることで実現される。このため、ユーザが所有する各再生装置が「正当」である条件を満たしていたとしても、ユーザが同じコンテンツを複数の再生装置に跨って利用したい場合には、個々の再生装置毎にライセンスを得る手続きをとる必要があり、操作が面倒になってしまう。あるいは同じコンテンツを利用するために、逐次課金されてしまうので、過大な対価を強いられることになる。

【００１８】

また、コンテンツの流通・配信事業が発展している昨今においては、複数のコンテンツ配信事業者によってさまざまなコンテンツが提供されている。しかしながら、ユーザが所有する各再生装置が「正当」であったとしても、個々の再生装置が異なるコンテンツ配信事業者にライセンス登録していた場合、同じユーザに帰属するにも拘らず、装置間に跨ってコンテンツを利用する（コンテンツを共有する）という融通性がないため、複数のコンテンツ配信事業者に登録した（又はアカウントを取得した）利益を十分に得ることができない。コンテンツ配信時業者側から見れば、事業協力が不十分であり顧客の利便性が低いと言わざるを得ない。

【００１９】

【発明が解決しようとする課題】

本発明の目的は、使用許諾など何らかの契約や利用条件に基づいてコンテンツの利用を好適に管理することができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することにある。

【００２０】

本発明のさらなる目的は、コンテンツの利用者にライセンスを与えることによりコンテンツの利用を制御しコンテンツの保護を好適に図ることができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することにある。

【００２１】

本発明のさらなる目的は、コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にすることができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することにある。

【００２２】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、ユーザのクライアントにコンテンツを配信するコンテンツ配信システムであって、ユーザは２以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

ユーザの各クライアントを登録して顧客関連情報を取得する登録手段と、

顧客関連情報を管理する顧客関連情報管理手段と、

クライアントからの要求に応じて該要求元クライアントへコンテンツを提供するコンテンツ提供手段と、

前記コンテンツ提供手段からコンテンツを取得したクライアントからの要求に応じて該要求元クライアントへ該取得コンテンツについてのライセンスを提供するライセンス提供手段と、

同一ユーザが持つ１つのクライアントから他のクライアントへのコンテンツの移動が正当であることを示すコンテンツ・コピー証明書を該移動元のクライアントに提供するコンテンツ・コピー証明書提供手段と、

を具備することを特徴とするコンテンツ配信システムである。

【００２３】

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する

機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

【００２４】

本発明の第１の側面に係るコンテンツ配信システムによれば、ユーザは、複数のクライアントを所持し、個々のクライアントが異なるライセンス・サーバに登録している場合であっても、１つのクライアント上でダウンロードしたコンテンツを他のクライアントに移動する際、コンテンツの移動先が正当であることを示すコンテンツ・コピー証明書を添付する。そして、移動先のクライアントではコンテンツ・コピー証明書を基に、受け取ったコンテンツを取り込み、再生する権利について正当であることを確認することができる。

【００２５】

すなわち、本発明の第１の側面に係るコンテンツ配信システムによれば、コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にすることができる。また、ユーザが複数のクライアント間でコンテンツを利用する作業的な負担が軽減され、コンテンツ配信サービスの利用が促進される。

【００２６】

このような複数のクライアント間でのコンテンツの共有は、コンテンツ配信事業者間の協業により実現される。コンテンツの移動元及び移動先となる各クライアントは、それぞれ別個のコンテンツ配信事業者に登録されていてもよい。このような場合、顧客関連情報提供手段によってコンテンツ配信事業者間で互いの顧客関連情報を照会できるようにして、コンテンツ移動元のクライアントを登録する配信事業者は、コンテンツ移動先のクライアントが同じユーザに所持されている正当な機器であることを照合処理するようにすればよい。

【００２７】

ここで、前記コンテンツ・コピー証明書提供手段は、移動先のクライアントに対するライセンスを含んだコンテンツ・コピー証明書を生成するようにしてもよい。このような場合、移動先のクライアントは、コンテンツ・コピー証明書からライセンスを取り出してコンテンツを利用することが可能である。したがって、

移動先のクライアント自身は、コンテンツ配信事業者に登録し直接ライセンスを取得するという作業が不要であり、コンテンツの共有を円滑に実現することができる。

【0028】

また、コンテンツ移動元及びコンテンツ移動先の各クライアントはそれぞれ異なるライセンス提供手段に登録され、各ライセンス提供手段は登録クライアントに対して自己の公開鍵を提供するようにしてもよい。このような場合、前記コンテンツ・コピー証明書提供手段は、コンテンツ移動先のクライアントが登録されているライセンス提供手段の秘密鍵を用いてコンテンツ・コピー証明書に電子署名を施すことにより、コンテンツ・コピー証明書の改竄を防止し、安全に移動することができる。また、移動先のクライアントは、その公開鍵を用いて復号し、コンテンツのライセンスを取り出すことができる。

【0029】

また、前記コンテンツ・コピー証明書提供手段は、前記移動元のクライアントから移動対象となるコンテンツについてのライセンスＩＤと移動先のクライアントのクライアントＩＤを取得し、さらに前記顧客関連情報関連手段に照会して、移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを確認してからコンテンツ・コピー証明書を提供するようにすることで、コンテンツ・コピー証明書の捏造や悪用を好適に防止することができる。

【0030】

また、前記顧客関連情報提供手段は、リーフＩＤとクライアントＩＤの対応テーブル、クライアントＩＤとクライアントの公開鍵証明書の対応テーブル、クライアントＩＤとユーザＩＤの対応テーブル、コンテンツＩＤとライセンスＩＤの対応テーブル、ユーザＩＤとダウンロードしたコンテンツのコンテンツＩＤの対応テーブル、ユーザＩＤとダウンロードしたライセンスのライセンスＩＤの対応テーブル、コンテンツ・コピー証明書の発行履歴を管理すればよい。

【0031】

ここで、前記顧客関連情報管理手段は、前記コンテンツ提供手段がクライアントにコンテンツを提供し、及び／又は、前記ライセンス提供手段がクライアントにライセンスを提供する度に顧客関連情報を更新するようにすればよい。

【００３２】

また、本発明の第１の側面に係るコンテンツ配信システムは、クライアントへのライセンス提供に応じてクライアントへの課金処理を行なう課金処理手段をさらに備えていてもよい。

【００３３】

そして、前記課金処理手段は、ライセンスを提供する場合とコンテンツ・コピー証明書を提供する場合とで差額を設けるようにてもよい。例えば、同じコンテンツについての２度目のライセンス提供に相当するコンテンツ・コピー証明書の料金を初期のライセンス取得よりも低額にし又は無料にすることにより、ユーザが複数のクライアント間でコンテンツを利用するコスト的な負担が軽減され、コンテンツ配信サービスの利用が促進される。

【００３４】

また、本発明の第２の側面は、コンテンツを使用するためのライセンスを提供する処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、ユーザは２以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

コンテンツ移動元のクライアントから移動対象となるコンテンツについてのライセンスＩＤとコンテンツ移動先のクライアントのクライアントＩＤを取得するステップと、

コンテンツ移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを判別するステップと、

コンテンツ・コピー証明書を作成するステップと、

コンテンツ・コピー証明書をコンテンツ移動元のクライアントに提供するステ

ップと、

を具備することを特徴とするコンピュータ・プログラムである。

【００３５】

本発明の第２の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第２の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係るコンテンツ配信システムと同様に、コンテンツの保護を確保しながら複数クライアント間でのコンテンツの共有を実現するという作用効果を得ることができる。

【００３６】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３７】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態について詳解する。

【００３８】

図１には、本発明の一実施形態に係るコンテンツ配信システムの構成例を模式的に示している。同図に示す例では、コンテンツ配信システムは、コンテンツを提供する配信事業者側と、顧客側に分かれて構成される。配信事業者と顧客の間は、例えばインターネットやその他の広帯域通信網（ｘＤＳＬ：x Digital Subscriber Line、CATV（Cable TV）、無線ネットワークなど）で相互接続されている。

【００３９】

コンテンツ配信事業者側は、図示の通り、配信事業者Ａ及びＢを始めとして、複数の配信事業者で構成されている。

【００４０】

各配信事業者は、顧客のコンテンツ再生装置（以下では、「クライアント」と

呼ぶ）毎にユーザ（クライアント）登録並びにコンテンツのライセンス供与を行なうライセンス・サーバと、提供すべきコンテンツの蓄積並びに配信処理を行なうコンテンツ・サーバと、ユーザ登録時及び／又はライセンス提供時（並びに、コンテンツ・コピー証明書（後述）発行時）に課金処理を行なう課金サーバと、顧客又はクライアントにコンテンツのライセンスを与えるために必要な各種データを保管する業務系データベース・サーバとを備えている。

【００４１】

本実施形態では、各配信事業者間は、例えばインターネットやその他のバックボーン通信網で相互接続されている。また、配信事業者間の事業協力を円滑に行なうために、配信事業者毎の業務系データベースを統括する業務系データベース・サーバＣ（ＤＢ　Ｃ）が構築されている。

【００４２】

各配信事業者毎に設置されている業務系データベース・サーバＡ（ＤＢ　Ａ）及び業務系データベース・サーバＢ（ＤＢ　Ｂ）は、自己に存在しないユーザ情報は業務系ＤＢ　Ｃに照会するとともに、更新内容を業務系ＤＢ　Ｃに反映させる同期処理を適宜行なうようにする。但し、業務系ＤＢ　Ｃは必須ではなく、業務系ＤＢ　Ａと業務系ＤＢ　Ｂの間で情報を共有できる何らかの仕組みが備わっていればよい。

【００４３】

なお、図１に示す例では、配信事業者Ａ及びＢがそれぞれ独自にライセンス・サーバ、課金サーバ、コンテンツ・サーバ、業務系データベース・サーバを構築・保有しているが、一部又は全部のサーバを配信事業者間で共同利用するようにしてもよいし、一方の配信事業者が保有するコンテンツ・サーバを他方の配信事業者が流用するようにしてもよい。

【００４４】

コンテンツ配信システム内では多数の顧客が存在するが、図１に示す例では図面の簡素化のため、単一の顧客のみ示している。図示の顧客は、クライアントＡ並びにクライアントＢを始め、複数のコンテンツ再生装置を所有し利用している。各クライアントは、ＤＲＭで言う「正当」の条件を備えており、暗号鍵やコン

テンツ鍵、並びに復号されたコンテンツを外部に漏らさないで処理することができる。

【0045】

図示の例では、クライアントAは、配信事業者Aに対して事前登録しており、配信事業者Aからコンテンツの提供並びにライセンスの取得を行なうことができる。また、クライアントBは、配信事業者Bに対して事前登録しており、配信事業所Bからコンテンツの提供並びにライセンスの取得を行なうことができる。

【0046】

クライアントAはライセンス・サーバAに対して事前登録並びにライセンス取得要求を行ない、クライアントBはライセンス・サーバBに対して事前登録並びにライセンス取得要求を行なう。ここで、ライセンス・サーバA及びBは、互いの秘密鍵を所持しているものとする。

【0047】

クライアントAからクライアントBへのコンテンツの移動は、例えばクライアントAでコンテンツ書き込み処理を行なった記録媒体をクライアントBに移動する他、パーソナル・ネットワークを利用してデータ伝送するなどの方法が挙げられる。但し、クライアントAからクライアントBへコンテンツを移動する際、移動元のクライアントAは、コンテンツを配信事業者から既に購入済み（又はライセンス取得済み）であるとする。

【0048】

本実施形態では、ユーザを特定するためにユーザＩＤを使用するが（後述）、各クライアント固体を特定するクライアントＩＤを代わりに使用することもできる。また、同一のユーザであっても、配信事業者による各サービスで個別にユーザＩＤが存在するが、それらのユーザＩＤが各業務系データベースを利用して関係付け（紐付け）されており、同一のユーザであることを各配信事業者が把握できるものとする。クライアントＩＤも業務系データベース・サーバA、B、及びCに管理されている。なお、本実施形態では、ユーザＩＤとパスワードによる認証を行なうようになっているが、クライアントＩＤ（機器ＩＤ）による認証（機器認証）や、機器認証とユーザ認証の組み合わせによりユーザ情報を取り扱うよ

うにしてもよい。

【００４９】

本実施形態に係るコンテンツ配信システムは、以下の事柄を前提条件として備えている。

【００５０】

①配信されたコンテンツは、配信事業者あるいはコンテンツの著作権を保有する者の意思によって、顧客によるコンテンツ利用範囲を制限することができる（著作権管理されている）環境が提供されている。

②この著作権管理環境では、暗号化されたコンテンツと、その暗号を解くライセンスを別物で扱うことができる。

③各クライアントが著作権管理・保護を確保するための情報処理方法を備えている（「正当」である）。

④それぞれのコンテンツ配信事業者から受信するクライアントは異なる。

⑤それぞれのクライアントは、受信したコンテンツをその受信クライアントあるいは受信クライアントに接続可能な記録媒体に保管することができる。

⑥各クライアント間においてコンテンツを共有する際、記録媒体や有線・無線通信によって顧客自らがクライアント間でコンテンツのやりとりを行なうことができる。

⑦それぞれのコンテンツ配信事業者が有する顧客関連情報（顧客自体の情報、顧客保有クライアントの情報、購入コンテンツの情報など）を交換又は共有することができる。

【００５１】

本実施形態に係るコンテンツ配信システムでは、かかる前提条件の下で、クライアントＡで取得したコンテンツをクライアントＢに保管する際に、クライアントＢの情報（クライアントの機器ＩＤなどを含んだ「コンテンツ・コピー証明書（後述）」）をそのコンテンツに付加し、クライアントＢを特定できるようにすることにより、コンテンツの保護を担保しながらクライアントＡ及びＢ間でのコンテンツの共有を実現することができる。但し、クライアントＡは、移動するコンテンツを配信事業者から既に購入済み（又はライセンス取得済み）である。コ

ンテンツを共有するための詳細な処理手順については後述に譲る。

【００５２】

図２には、本実施形態に係るコンテンツ配信システムにおいて、各種サーバあるいはクライアントとして動作するホスト装置のハードウェア構成を模式的に示している。

【００５３】

メイン・コントローラであるＣＰＵ（Central Processing Unit）１０１は、オペレーティング･システム（ＯＳ）の制御下で、各種のアプリケーションを実行する。本実施形態では、ホストがクライアント端末であればＣＰＵ１０１は、配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションを実行する。また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、ＣＰＵ１０１は各種のサーバ・アプリケーションを実行する。図示の通り、ＣＰＵ１０１は、バス１０８によって他の機器類（後述）と相互接続されている。

【００５４】

主メモリ１０２は、ＣＰＵ１０１において実行されるプログラム･コードをロードしたり、実行プログラムの作業データを一時保管したりするために使用される記憶装置であり、例えばＤＲＡＭ（Dynamic RAM）のような半導体メモリが使用される。ホストがクライアント端末であればＣＰＵ１０１は、配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションが実行プログラムとして主メモリ１０２にロードされる。また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、ＣＰＵ１０１は各種のサーバ・アプリケーションが実行プログラムとして種メモリ１０２にロードされる。

【００５５】

また、ＲＯＭ（Read Only Memory）１０３は、データを恒久的に格納する半導体メモリであり、例えば、起動時の自己診断テスト（ＰＯＳＴ：Power On Self

Test）や、ハードウェア入出力用のプログラム・コード（ＢＩＯＳ：Basic Input/Output System）などが書き込まれている。

【００５６】

ディスプレイ・コントローラ１０４は、ＣＰＵ１０１が発行する描画命令を実際に処理するための専用コントローラである。ディスプレイ・コントローラ１０３において処理された描画データは、例えばフレーム・バッファ（図示しない）に一旦書き込まれた後、ディスプレイ１１１によって画面出力される。ディスプレイ１１１の表示画面は、一般に、ユーザからの入力内容やその処理結果（より具体的にはコンテンツの再生画面）、あるいはエラーその他のシステム・メッセージをユーザに視覚的にフィードバックする役割を持つ。

【００５７】

入力機器インターフェース１０５は、キーボード１１２やマウス１１３、あるいはその他のユーザ入力機器を対話装置１００に接続するための装置である。

【００５８】

ネットワーク・インターフェース１０６は、Ｅｔｈｅｒｎｅｔ（登録商標）などの所定の通信プロトコルに従って、システム１００をＬＡＮ（Local Area Network）などの局所的ネットワーク、さらにはインターネットのような広域ネットワークに接続することができる。あるいは、車載端末などの場合には、携帯電話などの無線方式により広域ネットワークに接続するインターフェースであってもよい。

【００５９】

ネットワーク上では、複数のホスト端末（図示しない）がトランスペアレントな状態で接続され、分散コンピューティング環境が構築されている。ネットワーク上では、ソフトウェア・プログラムやデータ・コンテンツなどの配信サービスを行なうことができる。

【００６０】

例えば、ホストがクライアント端末であれば、コンテンツ配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションをダウンロードできる他、

コンテンツ配信事業者への事前登録、コンテンツ・サーバからのコンテンツのダウンロード、ライセンス・サーバからのコンテンツのライセンス取得、ライセンス取得に伴う課金処理などの手続きをネットワーク経由でダウンロードすることができる。また、コンパイル前のソース・プログラムやコンパイル処理後のオブジェクト･プログラムなどを、ネットワーク経由で実行することができる。また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、各種のサーバ・アプリケーションをネットワーク経由でダウンロードできる他、顧客のクライアント端末との事前登録、コンテンツ配信、ライセンス提供、ライセンス提供に伴う課金処理などの手続きをネットワーク経由で実行することができる。

【００６１】

外部機器インターフェース１０７は、ハード･ディスク･ドライブ（ＨＤＤ）１１４やメディア･ドライブ１１５などの外部装置をホスト１００に接続するための装置である。

【００６２】

ＨＤＤ１１４は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でＨＤＤ１１４上に置くことを、プログラムのシステムへの「インストール」と呼ぶ。通常、ＨＤＤ１１４には、ＣＰＵ１０１が実行すべきオペレーティング･システムのプログラム･コードや、アプリケーション･プログラム、デバイス･ドライバなどが不揮発的に格納されている。

【００６３】

例えば、ホストがクライアント端末であれば、コンテンツ配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションなどを、ＨＤＤ１１４上にインストールすることができる。また、コンテンツ配信事業者からダウンロードした（又は他のクライアント端末から記録媒体などを介して移動された）コンテンツやコンテンツのライセンスなどをＨＤＤ１１４上に蓄積することができる。

また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、各種のサーバ・アプリケーションをＨＤＤ１１４上にインストールすることができる他、コンテンツ配信業務に必要な顧客関連情報（顧客自体の情報、顧客保有クライアントの情報、購入コンテンツの情報など）をＨＤＤ１１４上に蓄積することができる。

【００６４】

メディア・ドライブ１１５は、ＣＤ（Compact Disc）やＭＯ（Magneto-Optical disc）、ＤＶＤ（Digital Versatile Disc）などの可搬型メディアを装填して、そのデータ記録面にアクセスするための装置である。

【００６５】

可搬型メディアは、主として、ソフトウェア・プログラムやデータ・ファイルなどをコンピュータ可読形式のデータとしてバックアップすることや、これらをシステム間で移動（すなわち販売・流通・配布を含む）する目的で使用される。例えば、コンテンツ配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションや各種のサーバ・アプリケーションなどを、これら可搬型メディアを利用して複数の機器間で物理的に流通・配布することができる。また、コンテンツ配信事業者からダウンロードしたコンテンツをクライアント端末間で移動するために可搬型メディアを利用することができる。また、コンテンツ配信業務に必要な顧客関連情報（顧客自体の情報、顧客保有クライアントの情報、購入コンテンツの情報など）を配信事業者間で交換又は共有するために可搬型メディアを利用することができる。

【００６６】

図３には、ホストがクライアントとして動作するときの機能構成を模式的に示している。同図に示すように、クライアントは、事前登録部と、コンテンツ・ダウンロード部と、コンテンツ蓄積部と、コンテンツ移動処理部と、ライセンス取得・管理部と、課金処理部と、コンテンツ再生処理部で構成される。図示の各機能モジュールは、実際にはＣＰＵ１０１が所定のプログラム・モジュールを実行するという形態で実現される。

【００６７】

事前登録部は、クライアント上で特定の配信事業者からコンテンツの提供を受けそのライセンスを取得する前提として、ライセンス・サーバとの間で事前登録処理を行なう。事前登録処理の詳細については後述に譲る。

【００６８】

コンテンツ・ダウンロード部は、事前登録を行なった配信事業者のコンテンツ・サーバから所望のコンテンツをダウンロードする処理を行なう。通常、ユーザはクライアントのブラウザ画面を介してコンテンツを選択した後、コンテンツのダウンロードが起動されるが、このような処理事態は周知なので、本明細書ではこれ以上説明しない。ダウンロードされたコンテンツは、コンテンツ蓄積部に格納される。

【００６９】

ライセンス取得・管理部は、コンテンツ・サーバからダウンロードしたコンテンツ、あるいはコンテンツ移動処理部を介して同一ユーザの他のクライアントから取得したコンテンツを利用するために必要なライセンスをライセンス・サーバから取得するとともに、取得したライセンス並びに事前登録時に取得した情報を管理する。

【００７０】

また、取得したライセンスの有効期限が既に切れている場合には、ライセンス取得・管理部は、ライセンス・サーバに対するライセンス更新処理を行なう。ライセンス取得処理並びにライセンス更新処理の詳細については、後述に譲る。

【００７１】

また、ダウンロードしたコンテンツを同一ユーザの別クライアントに移動（コピー）する場合には、ライセンス取得・管理部は、ライセンス・サーバに対してコンテンツ・コピー証明書の取得を行なう。また、一旦取り込んだコンテンツ・コピー証明書の通し番号を、「使用済みコンテンツ・コピー証明書」として記録する。コンテンツ・コピー証明書の取得処理の詳細については、後述に譲る。

【００７２】

また、ライセンス取得・管理部は、別クライアントからコンテンツ・コピー証

明書付きでコンテンツをコピーした際に、このコンテンツ・コピー証明書の中から取り出されたライセンスを保管する。

【００７３】

課金処理部は、配信時業者側の課金サーバに接続し、コンテンツ・サーバからダウンロードしたコンテンツ、あるいはコンテンツ移動処理部を介して同一ユーザの他のクライアントから取得したコンテンツを利用（コンテンツ再生）するためのライセンスを取得した対価、並びにコンテンツ・コピー証明書を取得した対価の支払い処理を実行する。

【００７４】

本実施形態では、コンテンツ・コピー証明書を取得時の代金は有料であっても無料であってもよい。また、有料の場合であっても、通常のライセンス取得時の料金に対して割り引いてもよい。これらの判断は、コンテンツ配信時業者側に委ねられ、課金サーバによって制御される。

【００７５】

コンテンツ再生処理部は、コンテンツ蓄積部から所望のコンテンツを取り出し、ライセンス取得・管理部に保管されている（又はコンテンツ・コピー証明書から取り出された）ライセンスを利用して、暗号化されているコンテンツ・データを復号並びにデコードし、その再生処理を行なう。コンテンツの再生処理は、音楽データを音響出力したり、映像データをディスプレイから表示出力したりすることを指す。

【００７６】

コンテンツ移動処理部は、同一ユーザ内の他のクライアントとの間でコンテンツの移動を行なう。他のクライアントへコンテンツを移動する場合には、コンテンツ移動処理部は、コンテンツ蓄積部から移動の対象となるコンテンツを取り出し、ライセンス・サーバから取得したコンテンツ・コピー証明書を付加して、可搬型の記録媒体に書き込んだり、あるいは有線・無線の通信路を経由して転送したりする。

【００７７】

また逆に、他のクライアントから移動したコンテンツを取り込む場合には、装

填された記録媒体からコンテンツを読み込んだり、有線・無線の通信路を経由してコンテンツを受信したりする。移動されたコンテンツはコンテンツ蓄積部に格納される。このとき、コンテンツ移動処理部は、コンテンツに付加されているコンテンツ・コピー証明書からライセンスを取り出し、これをライセンス取得・管理部に保管する。

【００７８】

図４には、ホストがライセンス・サーバとして動作するときの機能構成を模式的に示している。同図に示すように、ライセンス・サーバは、事前登録部と、ライセンス発行部と、ライセンス蓄積部と、データベース管理部とで構成される。図示の各機能モジュールは、実際にはＣＰＵ１０１が所定のプログラム・モジュールを実行するという形態で実現される。

【００７９】

事前登録部は、クライアントが当該配信事業者によるコンテンツ配信サービスを利用する前提として、クライアントの事前登録処理を行なう。事前登録処理の詳細については後述に譲る。

【００８０】

ライセンス蓄積部は、配信事業者が提供する各コンテンツに必要なライセンスを蓄積している。各ライセンスは、ライセンスＩＤなどのライセンス指定情報を利用して検索することができる。

【００８１】

ライセンス発行部は、クライアントが、ダウンロードしたコンテンツを利用する際に必要となるライセンスをライセンス蓄積部から取り出して、要求元のクライアントへ送信する。ライセンス発行部は、ライセンスの発行に伴い、クライアントへ課金を行なうため、課金サーバに通知する。ライセンス発行部は、ライセンスにリーフＩＤを付加する機能（ライセンス蓄積部より取り出したライセンスを加工する機能）も備えている。

【００８２】

また、ライセンス発行部は、ユーザがあるクライアントから別クライアントへコンテンツを移動する際に、コンテンツの移動が正当であることを証明するため

のコンテンツ・コピー証明書を発行し、コンテンツ移動元のクライアントへ送信する。ライセンス発行部は、コンテンツ・コピー証明書の発行に伴い、クライアントへ課金を行なうため、課金サーバに通知する。

【００８３】

本実施形態では、コンテンツ・コピー証明書を取得時の代金は有料であっても無料であってもよい。また、有料の場合であっても、通常のライセンス取得時の料金に対して割り引いてもよい。これらの判断は、コンテンツ配信時業者側に委ねられ、課金サーバによって制御される。

【００８４】

また、ライセンス発行部は、クライアント側からの有効期限の切れたライセンスの更新要求に応答して、ライセンスの更新処理も行なう。ライセンスの更新処理の詳細については後述に譲る。

【００８５】

データベース管理部は、事前登録部における事前登録の内容や、ライセンス発行部において発行したライセンス情報を業務系データベースへ登録・更新処理する。

【００８６】

図５には、ホストがコンテンツ・サーバとして動作するときの機能構成を模式的に示している。同図に示すように、コンテンツ・サーバは、送受信部と、配信コンテンツ蓄積部と、コンテンツ取出部と、暗号化部と、で構成される。図示の各機能モジュールは、実際にはＣＰＵ１０１が所定のプログラム・モジュールを実行するという形態で実現される。

【００８７】

送受信部は、クライアントからのコンテンツ要求（コンテンツの指定情報）を受信したり、指定されたコンテンツ・データを要求元クライアントに送信したりする処理を行なう。

【００８８】

配信コンテンツ蓄積部は、配信事業者において配信サービスを行なっているコンテンツ・データを保存・管理している。本実施形態では、コンテンツ・データ

はＡＴＲＡＣ（Adaptive Transform Acoustic Coding）３方式でエンコードされた状態で配信コンテンツ蓄積部に格納されている。

【００８９】

コンテンツ取出部は、送受信部で受信したコンテンツの指定情報を解析して、指定されたコンテンツを配信コンテンツ蓄積部から取り出して、暗号化部へ渡すようになっている。

【００９０】

暗号化部は、クライアントへ配信するコンテンツを、コンテンツ・キーＫｃを用いて暗号化する。

【００９１】

データベース管理部は、クライアントに対してコンテンツの配信サービスを行なった情報を業務系データベースへ登録・更新処理する。

【００９２】

コンテンツの共有処理の前に、クライアントＡ及びＢは、それぞれライセンス・サーバＡ及びＢにアクセスして事前登録処理を行なう。この事前登録処理を行なうことで、リーフＩＤ、ＤＮＫ（デバイス・ノード・キー）、各クライアントの秘密鍵及び公開鍵のペア、ライセンス・サーバの公開鍵、及び各公開鍵の証明書を含む「サービス・データ」を取得しておく。

【００９３】

ここで、リーフＩＤは、クライアント毎に割り当てられた識別情報を表わし、ＤＮＫは、そのライセンスに対応するＥＫＢ（有効化ブロック）に含まれる暗号化されているコンテンツ・キーK_cを復号するのに必要なデバイス・ノード・キーである。なお、ＤＮＫについては、本出願人に既に譲渡されているＷＯ　０２／０８０４４６号明細書に記述されているが、その詳細な仕組み自体は本発明の要旨に直接関連しないので、本明細書中では説明を省略する。

【００９４】

図６には、クライアントがライセンス・サーバに事前登録を行なうための処理手順をフローチャートの形式で示している。

【００９５】

クライアントは、自己の登録先となるコンテンツ配信事業者のライセンス・サーバに対して、サービス・データ要求を送信する（ステップＳ１）。

【００９６】

ライセンス・サーバは、クライアントからサービス・データ要求を受信すると、これに応答して、要求元クライアントにユーザ情報要求を送信する（ステップＳ１１）。

【００９７】

クライアントは、ユーザ情報要求を受信すると、ディスプレイなどにユーザ情報の入力を促すメッセージ並びにユーザ情報の入力画面を表示する（ステップＳ２）。そして、ユーザがキーボードやマウスなどの入力装置を介して、ユーザの個人情報や決済情報などのユーザ情報を入力すると、これをライセンス・サーバに送信する（ステップＳ３）。（本実施形態では、ユーザＩＤとパスワードによる認証を行なうようになっているが、クライアントＩＤ（機器ＩＤ）による認証（機器認証）や、機器認証とユーザ認証の組み合わせによりユーザ情報を取り扱うようにしてもよい。）

【００９８】

ライセンス・サーバは、ユーザ情報を受信すると、そのライセンス・サーバに割り当てられたカテゴリのノード以下のリーフのうち、未だ割り当てられていないリーフを要求元クライアントに割り当て、そのリーフからライセンス・サーバに割り当てられたカテゴリのノードまでのパス上のノードに割り当てられたノード・キーの組をデバイス・ノード・キーＤＮＫとして生成する。そして、生成されたＤＮＫと、クライアントに割り当てられたリーフのリーフＩＤと、クライアントの秘密鍵及び公開鍵のペアと、ライセンス・サーバの公開鍵及び公開鍵の証明書を含むサービス・データを生成する（ステップＳ１２）。そして、要求元クライアントに対して、このサービス・データを送信する（ステップＳ１３）。

【００９９】

また、ライセンス・サーバは、サービス・データの送信後、ユーザ情報をリーフＩＤに対応付けて記録しておくとともに、事前登録の内容を業務系データベースに登録する（ステップＳ１４）。

【0100】

クライアントは、ライセンス・サーバからサービス・データを受信すると、これを暗号化して、ライセンス取得・管理部において保管しておく（ステップS4）。

【0101】

以上のようにして、ライセンス・サーバはクライアント及びユーザを登録し、クライアントは所望のコンテンツ配信サービスを利用するために必要なデバイス・ノード・キーを含むサービス・データを受け取ることができる。

【0102】

本実施形態では、各配信事業者の業務系データベース・サーバA及びBは、顧客関連情報を管理するために、以下に示すような複数のテーブルを保有しており、コンテンツ・サーバなどの他のサブシステムは必要に応じてこれらのテーブルを利用（参照、追記、書き換えなど）することができる。

【0103】

（1）リーフIDとクライアントIDの対応テーブル

（2）クライアントIDとクライアントの公開鍵証明書の対応テーブル

（3）クライアントIDとユーザIDの対応テーブル

（4）ユーザIDとユーザ・パスワードの対応テーブル

（5）コンテンツIDとライセンスIDの対応テーブル

（6）ユーザIDとダウンロードしたコンテンツのコンテンツIDの対応テーブル（他にダウンロードした日時やライセンスIDなども記録することができる）

（7）ユーザIDとダウンロードしたライセンスのライセンスIDの対応テーブル（他にダウンロードした日時なども記録することができる）

（8）コンテンツ・コピー証明書の発行履歴

【0104】

また、業務系データベース・サーバCは、上記の業務系データベース・サーバA及びBに保管されている顧客関連情報のうち以下に示す情報を、配信事業者間で共有するために設置されており、双方の配信事業者A及びBは必要なときにその内容を参照したり更新したりすることができる。

【０１０５】

（１）リーフＩＤとクライアントＩＤの対応テーブル

（２）クライアントＩＤとクライアントの公開鍵証明書の対応テーブル

（３）クライアントＩＤとユーザＩＤの対応テーブル

（４）コンテンツＩＤとライセンスＩＤの対応テーブル

（５）ユーザＩＤとダウンロードしたコンテンツのコンテンツＩＤの対応テーブル（他にダウンロードした日時やライセンスＩＤなども記録することができる）

（６）ユーザＩＤとダウンロードしたライセンスのライセンスＩＤの対応テーブル（他にダウンロードした日時なども記録することができる）

【０１０６】

本実施形態に係るコンテンツ配信システムでは、クライアントＡで取得したコンテンツをクライアントＢに保管する際に、「コンテンツ・コピー証明書」をそのコンテンツに付加し、クライアントＢを特定できるようにすることにより、コンテンツの保護を担保しながらクライアントＡ及びＢ間でのコンテンツの共有を実現することができる。

【０１０７】

このコンテンツの共有は、図１に示すように以下の手順Ｐ１～Ｐ６に従って行なわれる。但し、クライアントＡは、移動するコンテンツを配信事業者から既に購入済み（又はライセンス取得済み）である。また、ライセンス・サーバＡ及びＢは互いの秘密鍵をあらかじめ記憶している。また、各クライアントのクライアントＩＤがユーザＩＤと対応付けて、業務系データベースに記録されている。

【０１０８】

Ｐ１：コンテンツのダウンロード

Ｐ２：ライセンスのダウンロードとコンテンツの再生

Ｐ３：業務系データベース間の情報更新

Ｐ４：コンテンツ・コピー証明書の発行

Ｐ５：コンテンツ及びコンテンツ・コピー証明書の記録媒体へのコピー

Ｐ６：コンテンツ取り込み処理

【０１０９】

以下、各段階に手順について説明する。

【０１１０】

コンテンツのダウンロード：

図７には、コンテンツをダウンロードする際のクライアントＡ側の処理手順をフローチャートの形式で示している。

【０１１１】

ユーザがディスプレイ画面をキーボードやマウスなどの入力装置を介して操作することによって、コンテンツのダウンロード処理が起動される。これに応答して、ネットワーク・インターフェース１０６を介して、コンテンツ・サーバＡへアクセスする（ステップＳ２１）。

【０１１２】

コンテンツ・サーバＡへアクセスした結果、クライアントのディスプレイ画面上には、コンテンツ選択画面（図示しない）が表示される。ユーザは、同画面上で、キーボードやマウスなどの入力装置を介して所望のコンテンツを指定する。そして、クライアントＡはコンテンツを指定する情報をコンテンツ・サーバＡへ通知する（ステップＳ２２）。さらに、コンテンツ・サーバＡに対してユーザＩＤを通知する（ステップＳ２３）。

【０１１３】

後述するように、コンテンツ・サーバＡは、コンテンツ指定情報の通知に応答して、該当するコンテンツを暗号化して送信してくる。クライアントＡは、暗号化コンテンツを受信して（ステップＳ２４）、これをコンテンツ蓄積部に格納する（ステップＳ２５）。

【０１１４】

また、図８には、コンテンツをダウンロードする際のコンテンツ・サーバ側の処理手順をフローチャートの形式で示している。

【０１１５】

コンテンツ・サーバＡは、クライアントＡよりアクセスを受けるまで待機する（ステップＳ３１）。そして、アクセスを受けたと判断すると、クライアントＡから送信されてきた、コンテンツを指定する情報を取り込む（ステップＳ３２）

。このコンテンツを指定する情報は、図６に示したフローチャートのステップＳ２２において、クライアントＡが通知してきた情報に該当する。

【０１１６】

次いで、コンテンツ・サーバＡは、蓄積しているコンテンツの中から、先行ステップＳ３２において取り込まれた情報で指定されたコンテンツを読み出す（ステップＳ３３）。

【０１１７】

そして、読み出されたコンテンツを、コンテンツ・キーＫｃを用いて暗号化する（ステップＳ３４）。配信コンテンツ蓄積部に記憶されている・コンテンツ・データは、既にＡＴＲＡＣ３方式によりエンコードされているので、このエンコードされたコンテンツ・データが暗号化されることになる。なお、コンテンツ・データをあらかじめ暗号化してから配信コンテンツ蓄積部に格納しておくことにより、ステップＳ３４を省略することができる。

【０１１８】

次いで、業務系データベースＡから、コンテンツＩＤに対応したライセンスＩＤを取り込む（ステップＳ３５）。そして、暗号化したコンテンツ・データを伝送するフォーマットを構成するヘッダに、暗号化コンテンツを復号するのに必要なキー情報（後述）と、コンテンツを利用するのに必要なライセンスを識別するライセンスＩＤを付加する（ステップＳ３６）。

【０１１９】

そして、ステップＳ３４において暗号化したコンテンツと、ステップＳ３６においてキーとライセンスＩＤを付加したヘッダとをフォーマット化したデータを、要求元のクライアントＡに送信する（ステップＳ３７）。

【０１２０】

最後に、クライアントＡのユーザＩＤと送信したコンテンツのコンテンツＩＤを業務系データベースＡに記録する（ステップＳ３８）。業務系データベースＡに記録した内容は、同期処理により業務系データベースＣにも反映されており、他方の配信事業者Ｂからも利用することができる。

【０１２１】

図９には、コンテンツ・サーバＡからクライアントＡにコンテンツを配信するときに用いられるデータ・フォーマットの構成例を示している。同図に示すように、このフォーマットは、ヘッダ（Ｈｅａｄｅｒ）とデータ（Ｄａｔａ）とで構成される。

【０１２２】

ヘッダには、コンテンツ情報（Content Information）と、ライセンスＩＤ（License ID）と、イネーブリング・キー・ブロック（有効化キー・ブロック：ＥＫＢ（Enabling Key Block））と、ＥＫＢから生成されたキーK_{EKB}を用いて暗号化されたコンテンツ・キーK_cとしてのデータK_{EKB}（K_c）が配置されている。なお、ＥＫＢに関しては、本出願人に既に譲渡されているＷＯ　０２／０８０４４６に記載されているが、本発明の要旨には直接関連しないので、本明細書中では説明を省略する。

【０１２３】

コンテンツ情報には、データとしてフォーマット化されているコンテンツ・データを識別するための識別情報としてのコンテンツＩＤ（ＣＩＤ）と、そのコンテンツのコーデックの方式などの情報が含まれている。

【０１２４】

データは、任意の数の暗号化ブロック（Encryption Block）により構成される。各暗号化ブロックは、イニシャル・ベクトル（ＩＶ：Initial Vector）と、シード（Ｓｅｅｄ）と、コンテンツ・データをキーK'_cで暗号化したデータ$E_{K'c}$（Ｄａｔａ）とで構成される。

【０１２５】

キーK'_cは、以下の式により示されるように、コンテンツ・キーK_cと、乱数で設定されるシードにハッシュ関数を適用して演算された値で構成される。

【０１２６】

【数１】

$$K'_c = Hash(K_c, Seed)$$

【０１２７】

イニシャル・ベクトルＩＶとシードＳｅｅｄは、各暗号化ブロック毎に異なる

値に設定される。

【０１２８】

この暗号化は、コンテンツのデータを８バイト単位で区分して、８バイト毎に行なわれる。後段の８バイトの暗号化は、前段の８バイトの暗号化の結果を利用して行なわれるＣＢＣ（Cipher Block Chaining）モードで行なわれる。

【０１２９】

ＣＢＣモードの場合、最初の８バイトのコンテンツ・データを暗号化するとき、その前段の８バイトの暗号化の結果が存在しないため、最初の８バイトのコンテンツ・データを暗号化するときはイニシャル・ベクトルＩＶを初期値として暗号化が行なわれる。

【０１３０】

このＣＢＣモードによる暗号化を行なうことで、１つの暗号化ブロックが解読されたとしても、その影響が他の暗号化ブロックに及ぶことが抑制される。なお、この暗号化の処理手順に関しては本出願人に既に譲渡されているＷＯ　０２／０８０４４６に記載されているが、本発明の要旨には直接関連しないので、本明細書中ではこれ以上説明しない。また、暗号化方式については、これに限らず、単にコンテンツ・キーK_cでコンテンツ・データを暗号化するように構成してもよい。

【０１３１】

以上のようにして、クライアントＡは、コンテンツ・サーバＡからコンテンツを自由に取得することができる。コンテンツを利用（再生）するためにはコンテンツのライセンスを別途取得する必要があることから、本実施形態では、コンテンツの配信自体は無料とし、ライセンスの取得を有料にしている。したがって、コンテンツそのものは無料で、大量に配布することが可能である。

【０１３２】

ライセンスのダウンロードとコンテンツの再生：

図１０には、クライアントＡ側でダウンロードしたコンテンツを再生するための処理手順をフローチャートの形式で示している。

【０１３３】

まず、クライアントＡは、ユーザがキーボードやマウスなどの入力装置の操作を介して指示したコンテンツの識別情報（ＣＩＤ）を取得する（ステップＳ４１）。この識別情報は、例えば、コンテンツのタイトルや、記憶されているコンテンツ毎に付与されている番号などで構成される。

【０１３４】

コンテンツが指示されると、次いで、そのコンテンツに対応するライセンスＩＤ（そのコンテンツを使用するのに必要なライセンスの識別情報）を読み取る。このライセンスＩＤは、図９に示したように、暗号化されているコンテンツ・データのヘッダに記述されている。

【０１３５】

次いで、読み取られたライセンスＩＤに対応するライセンスが、クライアントにより既に取得され、ライセンス取得・管理部に保管されているかどうかを判断する（ステップＳ４２）。ここで、該当するライセンスが未だ取得されていない場合には、ステップＳ４３に進み、ライセンス取得処理（後述）を実行する。

【０１３６】

ステップＳ４２において、ライセンスが既に取得されていると判断された場合、あるいはステップＳ４３においてライセンス取得処理が実行された結果、ライセンスが取得された場合、さらに、取得されているライセンスが有効期限内かどうかを判断する（ステップＳ４４）。ライセンスが有効期限内のものであるかどうかは、ライセンスの内容として規定されている期限（後述）と、クライアントのシステム・タイマにより計時されている現在日時と比較することで判断される。

【０１３７】

ライセンスの有効期限が既に満了していると判断された場合には、ステップＳ４５に進み、ライセンスの更新処理（後述）を実行する。

【０１３８】

ステップＳ４４において、ライセンスが有効期限内であると判断された場合、あるいはステップＳ４５においてライセンスが更新された場合、さらにライセンスが正当であるかどうかを判断する（ステップＳ４６）。ライセンスの有効性は

、ライセンスに含まれている電子署名（後述）を利用して実行することができる。ライセンスが正当でない場合には、エラー処理を行なってから（ステップＳ４７）、本処理ルーチン全体を終了する。エラー処理は、正当なライセンスを改めて取得する処理であってもよい。

【０１３９】

ステップＳ４６において、ライセンスが正当であると判断された場合、該当する暗号化コンテンツ・データをコンテンツ蓄積部から読み出す（ステップＳ４８）。そして、暗号化されているコンテンツ・データを、図９に示したデータに配置されている暗号化ブロック単位で、コンテンツ・キーK_cを用いて復号する（ステップＳ４９）。

【０１４０】

さらに、復号されたコンテンツ・データをデコードし、コンテンツの再生処理を行なう（ステップＳ５０）。コンテンツの再生処理は、音楽データを音響出力したり、映像データをディスプレイから表示出力したりすることを指す。

【０１４１】

図１１には、図１０に示すフローチャート中のステップＳ４３で実行されるライセンス取得処理の詳細な手順をフローチャートの形式で示している。

【０１４２】

クライアントＡは、事前にライセンス・サーバＡにアクセスして登録処理を行なうことにより、リーフＩＤ、ＤＮＫ（デバイス・ノード・キー）、クライアントＡの秘密鍵及び公開鍵のペア、ライセンス・サーバの公開鍵、及び公開鍵の証明書を含むサービス・データを取得している（前述及び図６を参照のこと）。

【０１４３】

ここで、リーフＩＤは、クライアント毎に割り当てられた識別情報を表わし、ＤＮＫは、そのライセンスに対応するＥＫＢ（有効化ブロック）に含まれる暗号化されているコンテンツ・キーK_cを復号するのに必要なデバイス・ノード・キーである。

【０１４４】

まず、クライアントＡは、ユーザのキーボードやマウスなどの入力装置の操作

を介して、更新するライセンスの指定情報、並びにユーザＩＤとパスワードを入力する（ステップＳ６１，Ｓ６２）。

【０１４５】

次いで、クライアントＡは、入力されたユーザＩＤとパスワード、ライセンス指定情報、並びにサービス・データに含まれるリーフＩＤを含むライセンス要求を、ライセンス・サーバＢに送信する（ステップＳ６３）。

【０１４６】

ライセンス・サーバＡは、ユーザＩＤとパスワード、並びにライセンス指定情報に基づいてライセンスを発行し、要求元のクライアントＡに送信する。ライセンス・サーバＡによるライセンスの提供処理の詳細については後述に譲る。

【０１４７】

クライアントＡは、ライセンス・サーバＡからライセンスを受信することができた場合には（ステップＳ６４）、ライセンス取得・管理部においてそのライセンスを記憶する（ステップＳ６５）。

【０１４８】

他方、ライセンス・サーバＡからライセンスを受信することができない場合には（ステップＳ６４）、所定のエラー処理を実行して（ステップＳ６６）、本処理ルーチン全体を終了する。ここで言うエラー処理は、例えば、コンテンツを利用するためのライセンスが得られないので、コンテンツ再生処理部の起動を禁止する動作などが挙げられる。

【０１４９】

以上のようにして、クライアントＡは、コンテンツ・データに付随しているライセンスＩＤに対応するライセンスを取得して、初めてそのコンテンツを使用することが可能になる。

【０１５０】

なお、図１１に示すようなライセンス取得処理は、コンテンツのダウンロード後ではなく、その前に行なっておくことも可能である。

【０１５１】

図１２には、ライセンス・サーバからクライアントに提供されるライセンスの

データ構造を模式的に示している。同図に示すように、ライセンスは、使用条件、リーフＩＤやライセンス・サーバの電子署名などを含んでいる。

【０１５２】

使用条件には、そのライセンスに基づいてコンテンツを使用することが可能な使用期限、そのライセンスに基づいてコンテンツをダウンロードすることが可能なダウンロード期限、そのライセンスに基づいてコンテンツをコピーすることが可能な回数（許容されるコピー回数）、チェックアウト回数、最大チェックアウト回数、そのライセンスに基づいてコンテンツをＣＤ－Ｒなどの記録媒体に記録することができる権利、可搬型の記録媒体にコピーすることができる回数、ライセンスを所有権（買い取り状態）に移行できる権利、使用ログを取る義務などを示す情報などが含まれている。

【０１５３】

図１３には、クライアントＡ側からのライセンス要求（図１１に示すフローチャート中のステップＳ６３）に対応して実行される、ライセンス・サーバＡがクライアントＡにライセンスを提供するための処理手順をフローチャートの形式で示している。

【０１５４】

ライセンス・サーバＡは、クライアントＡからアクセスを受けるまで待機する（ステップＳ７１）。そして、クライアントＡからアクセスを受けたときに、クライアントＡに対して、ユーザＩＤとパスワード、並びにライセンスＩＤの送信を要求する。これに対し、クライアントＡからは、ステップＳ６３の処理として、ユーザＩＤとパスワード、リーフＩＤ並びにライセンス指定情報（ライセンスＩＤ）を送信するので、ライセンス・サーバＡ側ではこれらを取り込む（ステップＳ７２）。

【０１５５】

次いで、ライセンス・サーバＡは、業務系データベース・サーバＡに対して、ユーザＩＤとパスワードの照合処理を依頼し（ステップＳ７３）、クライアントＡの正当性をチェックする（ステップＳ７４）。ここで、照合に失敗した場合には、所定のエラー処理を実行して（ステップＳ７５）、本処理ルーチン全体を終

了する。この場合、クライアントＡに対してライセンスは発行されない。

【０１５６】

一方、照合処理が成功裏に終了した場合には、ライセンス・サーバＡは、さらに課金サーバＡにアクセスして、与信処理を依頼する（ステップＳ７６）。課金サーバＡは、ライセンス・サーバＡからの与信処理の要求に応答して、そのユーザＩＤとパスワードに対応する過去の支払い履歴などを調査し、そのユーザが過去にライセンスの対価の不払いなど好ましくない実績があるかどうかをチェックする（ステップＳ７７）。

【０１５７】

ここで、好ましくない支払い実績があるなど与信が妥当でないと判断された場合には、課金サーバＡは、ライセンス付与を不許可とする与信結果をライセンス・サーバＡに返信する。ライセンス・サーバＡは、これに応答して所定のエラー処理を実行して（ステップＳ７８）、本処理ルーチン全体を終了する。この場合、クライアントＡに対してライセンスは発行されない。

【０１５８】

一方、与信ＯＫであれば、次いで、ライセンス指定情報に対応するライセンスをライセンス蓄積部から取り出す（ステップＳ７９）。ライセンス蓄積部に格納されているライセンスは、あらかじめライセンスＩＤ、バージョン、作成日時、有効期限などの情報が記述されている。

【０１５９】

ライセンス・サーバＡは、取り出したライセンスにリーフＩＤを付加する（ステップＳ８０）。

【０１６０】

次いで、ライセンス・サーバＡは、このライセンスに対応付けられている使用条件を選択する（ステップＳ８１）。あるいは、ライセンス要求時にユーザから使用条件が指定されている場合には、その使用条件が必要に応じてあらかじめ用意されている使用条件に付加される。そして、選択された使用条件をライセンスに付加する。

【０１６１】

次いで、ライセンス・サーバＡは、自身の秘密鍵によりライセンスに電子署名を施すことで、図１２に示したようなライセンスを生成する（ステップＳ８２）。そして、このライセンスを要求元のクライアントＡに送信する（ステップＳ８３）。

【０１６２】

次いで、ライセンス・サーバＡは、いま送信したライセンス（使用条件、リーフＩＤを含む）をユーザＩＤとパスワードに対応付けて記憶しておく。また、業務系データベース・サーバＡにアクセスして、送信したライセンスのライセンスＩＤをユーザＩＤに対応付けて記録する（ステップＳ８４）。業務系データベースＡに記録した内容は、同期処理により業務系データベースＣにも反映されており、他方の配信事業者Ｂからも利用することができる。

【０１６３】

最後に、ライセンス・サーバＡは、課金サーバＡにアクセスして、ユーザＩＤとパスワードに対応するユーザに対する課金処理を実行する（ステップＳ８５）。課金サーバＡは、この課金処理の要求に応答して、該当するユーザに対する課金処理を実行する。課金サーバＡは、クレジット・カードなどを用いた信用決済やデビット・カードを用いた即時決済、電子マネーによる支払い、現金払いや金融機関への振込みなどに対応してもよい。但し、課金処理の形態は本発明の要旨に直接関連しないので、本明細書ではこれ以上説明しない。

【０１６４】

なお、課金処理に対してユーザが支払いを行なわなかったような場合には、そのユーザは与信を失い、以後ライセンスの付与を要求したとしてもライセンスを受けることができないことになる。すなわち、ユーザが与信を失った場合には、上述したように、課金サーバからライセンスの付与を不許可とする与信結果が返されるので、ライセンス・サーバはステップＳ７８においてエラー処理を実行する。エラー処理では、例えば要求元のクライアントに対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了する。また、要求元のクライアントでは、ライセンスを受けることができないので、すなわちコンテンツを利用すること（暗号を復号すること）ができないことになる。

【０１６５】

図１４には、図１０に示すフローチャート中のステップＳ４５において、クライアントが実行する、ライセンス・サーバに対するライセンスの更新処理の詳細な手順をフローチャートの形式で示している。

【０１６６】

まず、クライアントＡは、ユーザのキーボードやマウスなどの入力装置の操作を介して、ライセンス指定情報、ユーザＩＤ、及びパスワードを入力する（ステップＳ９１，Ｓ９２）。

【０１６７】

次いで、クライアントＡは、入力されたユーザＩＤとパスワード、並びにライセンス指定情報を含むライセンス更新要求を、ライセンス・サーバに送信する（ステップＳ９３）。

【０１６８】

ライセンス・サーバＡ側では、ライセンス更新要求に応答して、使用条件を提示してくる（後述）。これに対し、クライアントＡは、提示された使用条件を受信し、これをユーザに表示出力する（ステップＳ９４）。

【０１６９】

ユーザは、キーボードやマウスなどの入力装置を操作して、画面表示されている使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。このようにして選択された使用条件（すなわちライセンスを更新する条件）を購入するための申し込みを、ライセンス・サーバＡに送信する（ステップＳ９５）。

【０１７０】

ライセンス・サーバＡ側では、クライアントＡからの購入申し込みに応答して、最終的な使用条件を送信してくる（後述）。これに対し、クライアントＡは、ライセンス・サーバＡからの使用条件を受信して（ステップＳ９６）、これを対応するライセンスの使用条件として更新する（ステップＳ９７）。

【０１７１】

また、図１５には、図１０に示すフローチャート中のステップＳ４５（図１４

）に対応してライセンス・サーバで実行される、有効期限の切れたライセンスを更新するための詳細な処理手順をフローチャートの形式で示している。

【０１７２】

ライセンス・サーバＡは、クライアントＡからのアクセスを受けると（ステップＳ１０１）、クライアントＡが送信したライセンス更新要求（前述）を受信する（ステップＳ１０２）。

【０１７３】

そして、ライセンス・サーバＡは、更新要求されているライセンスに対応する使用条件（更新する使用条件）をライセンス蓄積部から読み出し、これを要求元のクライアントＡに送信する（ステップＳ１０３）。

【０１７４】

クライアントＡ側では、受信した使用条件をユーザに表示出力する。そして、ユーザは、キーボードやマウスなどの入力装置を操作して、画面表示されている使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。このようにして選択された使用条件（すなわちライセンスを更新する条件）を購入するための申し込みを、ライセンス・サーバＡに送信する（前述）。

【０１７５】

ライセンス・サーバＡは、クライアントＡからの使用条件の購入が申し込まれると、申し込まれた使用条件に対応するデータを生成し、クライアントＡに送信する（ステップＳ１０４）。クライアントＡ側では、ライセンス・サーバＡからの使用条件を受信して、これを対応するライセンスの使用条件として更新する（前述）。

【０１７６】

ここで、クライアントが、ライセンス・サーバから供給されたライセンスに基づいて、コンテンツ・サーバから供給されたコンテンツを利用する処理の仕組みについて、図２１を参照しながらまとめておく。

【０１７７】

コンテンツ・サーバからクライアントに対してコンテンツが提供されるととも

に、ライセンス・サーバからクライアントにライセンスが供給される。コンテンツは、コンテンツ・キーＫｃにより暗号化されており（Ｅｎｃ（K_c，Ｃｏｎｔｅｎｔ））、コンテンツ・キーＫｃは、ルート・キーＫＲ（ＥＫＢから得られるキーであって、図９に示したコンテンツ・データ中のキーK_{EKBC}に対応する）で暗号化され（Ｅｎｃ（ＫＲ，K_c））、ＥＫＢとともに、暗号化されてコンテンツに吹かされて要求元クライアントに提供される。

【０１７８】

図２１に示した例におけるＥＫＢには、例えば図２２に示すように、ＤＮＫで復号可能なルート・キーＫＲが含まれている（Ｅｎｃ（ＤＮＫ，ＫＲ））。したがって、クライアントは、サービス・データに含まれるＤＮＫを利用して、ＥＫＢからルート・キーＫＲを得ることができる。さらに、ルート・キーＫＲを用いて、Ｅｎｃ（ＫＲ，K_c）からコンテンツ・キーK_cを復号することができ、このコンテンツ・キーK_cを用いて、暗号化コンテンツＥｎｃ（K_c，Ｃｏｎｔｅｎｔ）からコンテンツを復号することができる。

【０１７９】

業務系データベース間の情報更新：

クライアントＡとコンテンツ配信事業者Ａの間でコンテンツやライセンスのダウンロードが行なわれると、その情報が配信事業者Ａ内の業務系データベースＡに記録される。本実施形態に係るコンテンツ配信システムでは、配信事業者Ａ及び配信事業者Ｂ間での事業協力により同一顧客のクライアントＡ及びクライアントＢ間でのコンテンツの共有を実現するために、業務系データベースＡの更新情報を業務系データベースＣに反映させて、配信事業者Ｂからも利用可能にする。

【０１８０】

配信事業者Ａからクライアントへ、コンテンツ又はライセンスのダウンロードが終了すると、業務系データベースＡ及びＣでは、以下に示す各テーブルの該当するエントリーが更新される。

【０１８１】

（１）リーフＩＤとクライアントＩＤの対応テーブル

（２）クライアントＩＤとクライアントの公開鍵証明書の対応テーブル

（３）クライアントＩＤとユーザＩＤの対応テーブル

（４）コンテンツＩＤとライセンスＩＤの対応テーブル

（５）ユーザＩＤとダウンロードしたコンテンツのコンテンツＩＤの対応テーブル（他にダウンロードした日時やライセンスＩＤなども記録することができる）

（６）ユーザＩＤとダウンロードしたライセンスのライセンスＩＤの対応テーブル（他にダウンロードした日時なども記録することができる）

【０１８２】

コンテンツ・コピー証明書の発行：

この時点で、クライアントＡは、移動するコンテンツを配信事業者から既に購入済み（又はライセンス取得済み）である。クライアントＡにダウンロードしたコンテンツをクライアントＢにおいて利用するために、別クライアントへコンテンツをコピーする許可書に相当する「コンテンツ・コピー証明書」を取得する。

【０１８３】

図１６には、クライアントＡがライセンス・サーバＡからコンテンツ・コピー証明書を取得するための処理手順をフローチャートの形式で示している。

【０１８４】

ユーザがディスプレイ画面をキーボードやマウスなどの入力装置を介して操作することによって、コンテンツのコピー証明書の発行処理が起動される。これに応答して、ネットワーク・インターフェース１０６を介して、ライセンス・サーバＡへアクセスする（ステップＳ１１１）。

【０１８５】

ライセンス・サーバＡへアクセスした結果、クライアントのディスプレイ画面上には、コンテンツ選択画面（図示しない）が表示される。ユーザは、同画面上で、キーボードやマウスなどの入力装置を介して所望のコンテンツを指定するとともに、ライセンスＩＤ、コピー先となるクライアント（この場合はクライアントＢ）のクライアントＩＤを入力する。そして、クライアントＡは、コンテンツを指定する情報を、ライセンスＩＤと、コピー先のクライアントＩＤとともにライセンス・サーバＡへ通知する（ステップＳ１１２）。さらに、ライセンス・サーバＡに対して、自己のユーザＩＤ及びパスワードを通知する（ステップＳ１１

３）。

【０１８６】

これに対し、ライセンス・サーバＡは、コンテンツ・コピー証明書を発行して、これをクライアントＡに返信する。そして、クライアントＡは、送られてきたコンテンツ・コピー証明書を受信し（ステップＳ１１４）、これを一旦記憶する（ステップＳ１１５）。

【０１８７】

また、図１７には、ライセンス・サーバＡがクライアントＡからの要求に応答してコンテンツ・コピー証明書を発行するための処理手順をフローチャートの形式で示している。

【０１８８】

ライセンス・サーバＡは、クライアントＡからアクセスを受けるまで待機する（ステップＳ１２１）。そして、クライアントＡからアクセスを受けたときに、クライアントＡに対して、コンテンツを指定する情報、ライセンスＩＤ、ユーザＩＤとパスワード、コピー先のクライアントＩＤの送信を要求する。これに対し、クライアントＡからは、ステップＳ１１２及びＳ１１３の処理として、これらの情報を送信するので、ライセンス・サーバＡ側ではこれらを取り込む（ステップＳ１２２）。

【０１８９】

次いで、ライセンス・サーバＡは、業務系データベース・サーバＡに対して、ユーザＩＤとパスワードの照合処理を依頼し（ステップＳ１２３）、クライアントＡの正当性をチェックする（ステップＳ１２４）。ここで、照合に失敗した場合には、所定のエラー処理を実行して（ステップＳ１２５）、本処理ルーチン全体を終了する。この場合、クライアントＡに対してコンテンツ・コピー証明書は発行されない。

【０１９０】

一方、ステップＳ１２４の照合処理が成功裏に終了した場合には、さらに業務系データベース・サーバＡに対して、クライアントＡが指定されたコンテンツを既に購入済みか（ライセンスを取得済みか）どうか、照合処理を依頼し（ステッ

プＳ１２６）、クライアントＡが当該コンテンツを購入済かどうかをチェックする（ステップＳ１２７）。ここで、照合に失敗した場合には、所定のエラー処理を実行して（ステップＳ１２８）、本処理ルーチン全体を終了する。この場合、クライアントＡに対してコンテンツ・コピー証明書は発行されない。なお、ステップＳ１２７におけるエラー処理は、正当なライセンスを改めて取得する処理であってもよい。

【０１９１】

ステップＳ１２７の照合処理が成功裏に終了した場合、今度は業務系データベース・サーバＣに対して、クライアントＡのユーザが、ステップＳ１２２で受信したクライアントＩＤで示されるクライアントＢを実際に所持しているかどうか、照合処理を依頼し（ステップＳ１２９）、同一ユーザがクライアントＢを所持するかどうかをチェックする（ステップＳ１３０）。ここで、照合に失敗した場合には、所定のエラー処理を実行して（ステップＳ１３１）、本処理ルーチン全体を終了する。この場合、クライアントＡに対してコンテンツ・コピー証明書は発行されない。なお、ステップＳ１３１におけるエラー処理は、クライアントＢを改めて事前登録する処理であってもよい。

【０１９２】

ステップＳ１３０における照合処理が成功裏に終了した場合は、さらに、業務系データベース・サーバＡに対して、コンテンツ・コピー証明書、すなわち要求元のクライアントＡから当該コンテンツをクライアントＢにコピーする許可書を発行してもよいかどうか、確認処理を依頼し（ステップＳ１３２）、コンテンツ・コピー証明書の発行の是非をチェックする（ステップＳ１３３）。ここで、確認処理に失敗した場合には、所定のエラー処理を実行して（ステップＳ１３４）、本処理ルーチン全体を終了する。この場合、クライアントＡに対してコンテンツ・コピー証明書は発行されない。

【０１９３】

一方、ステップＳ１３３における確認処理が成功裏に終了した場合には、業務系データベース・サーバＣにアクセスして、クライアントＢのリーフＩＤを取得する（ステップＳ１３５）。次いで、ステップＳ１２２で取得したライセンスＩ

Ｄに対応したライセンス情報を取得する（ステップＳ１３６）。そして、取得したライセンス情報とクライアントＢのリーフＩＤを基に、クライアントＢが当該コンテンツを利用することを許可するライセンスを作成する（ステップＳ１３７）。作成されたライセンスの構造は、図１２に示した通りである。

【０１９４】

次いで、ライセンス・サーバＡは、このライセンスに対して、ライセンス・サーバＢの秘密鍵で電子署名を施す（ステップＳ１３８）。

【０１９５】

次いで、ステップＳ１２２において取得した情報を用いて、コンテンツ・コピー証明書を作成し、これにライセンス・サーバＢの秘密鍵を用いて電子署名を施す（ステップＳ１３９）。ライセンス・サーバＡ及びＢは、互いの秘密鍵を所持している（前述）。

【０１９６】

次いで、ライセンス・サーバＡ電子署名が施されたコンテンツ・コピー証明書を、要求元のクライアントＡに送信する（ステップＳ１４０）。

【０１９７】

そして、最後に、業務系データベース・サーバＡにアクセスして、送信したコンテンツ・コピー証明書と対応するコンテンツＩＤ、ユーザＩＤ、コピー先となるクライアントＢのリーフＩＤに対応付けて記録する（ステップＳ１４１）。業務系データベースＡに記録した内容は、同期処理により業務系データベースＣにも反映されており、他方の配信事業者Ｂからも利用することができる。

【０１９８】

本実施形態では、コンテンツ・コピー証明書を取得時の代金は有料であっても無料であってもよい。また、有料の場合であっても、通常のライセンス取得時の料金に対して割り引いてもよい。これらの判断は、コンテンツ配信時業者側に委ねられ、課金サーバによって制御される。

【０１９９】

コンテンツ・コピー証明書の発行を有料で行なう場合、例えばステップＳ１３９とステップＳ１４０の間に課金処理が挿入される。このときの課金処理につい

て以下に説明する。

【０２００】

ライセンス・サーバＡは、課金サーバＡにアクセスして、与信処理を依頼する。課金サーバＡは、ライセンス・サーバＡからの与信処理の要求に応答して、そのユーザＩＤとパスワードに対応する過去の支払い履歴などを調査し、そのユーザが過去にライセンスの対価の不払いなど好ましくない実績があるかどうかをチェックする。与信ＯＫであれば、ユーザＩＤとパスワードに対応するユーザに対する課金処理を実行する。

【０２０１】

他方、好ましくない支払い実績があるなど与信が妥当でないと判断された場合には、課金サーバＡは、コンテンツ・コピー証明書の付与を不許可とする与信結果をライセンス・サーバＡに返信する。ライセンス・サーバＡは、これに応答して所定のエラー処理を実行して、本処理ルーチン全体を終了する。この場合、クライアントＡに対してコンテンツ・コピー証明書は発行されない。

【０２０２】

図１８には、ライセンス・サーバにより発行されるコンテンツ・コピー証明書のデータ構造を模式的に示している。同図に示すように、コンテンツ・コピー証明書は、当該証明書の通し番号と、コピー対象となるコンテンツのコンテンツＩＤと、ライセンスと、電子署名などで構成される。

【０２０３】

ライセンスは、コピー先となるクライアント（この場合はクライアントＢ）を登録するライセンス・サーバ（この場合はライセンス・サーバＢ）の秘密鍵で電子署名が施されている（前述）。

【０２０４】

電子署名は、証明書の通し番号、コンテンツＩＤ、及びライセンスの３つの値に対し、ライセンス・サーバＢの秘密鍵を用いて作成される。

【０２０５】

ライセンス及び電子署名がライセンス・サーバＢの秘密鍵で署名されていることから、コピー先のクライアントＢは、ライセンス・サーバＢの公開鍵を用いて

復号することができる。

【０２０６】

コンテンツ及びコンテンツ・コピー証明書の記録媒体へのコピー：

クライアントＡにダウンロードしたコンテンツを、クライアントＢにおいて利用するために、コンテンツ・コピー証明書を付加してコンテンツを移動する。

【０２０７】

図１に示す例では、クライアントＡにおいて、ダウンロードしたコンテンツを可搬型の記録媒体にコピーして、これをクライアントＢに装填することによってコンテンツの移動を行なう。

【０２０８】

この場合、クライアントＡ側では、コンテンツ蓄積部からコンテンツを取り出して、これを記録媒体に書き込むという処理が行なわれる。また、クライアントＢ側では、記録媒体に記録されたコンテンツを読み出してコンテンツ蓄積部に格納するという処理が行なわれる。

【０２０９】

勿論、ライセンスのないコンテンツを別のクライアントに移動する方法は、これに限定されるものではない。例えば、記録媒体以外に、有線・無線通信によってユーザ自らがクライアント間でのコンテンツのやりとりを行なってもよい。あるいは、一方のクライアントでコンテンツを購入すると、コンテンツ配信事業者が、同じユーザが保有する別のクライアントへも自動配信を行なうようにしてもよい。

【０２１０】

図１９には、クライアント間でコンテンツを移動する際の、移動元となるクライアントＡ側で行なう処理手順をフローチャートの形式で示している。

【０２１１】

まず、移動対象となるコンテンツ・データをコンテンツ蓄積部から取り出して、記録媒体へコピーする（ステップＳ１５１）。

【０２１２】

次いで、上述した処理手続きに従って取得したコンテンツ・コピー証明書を、

記録媒体へコピーする（ステップＳ１５２）。

【０２１３】

そして、クライアントＡ内のコンテンツ・コピー証明書を削除しておく（ステップＳ１５３）。

【０２１４】

なお、コンテンツ・コピー証明書の削除処理は、証明書の無断の複製や不正利用を防止するためであり、セキュリティ上問題がなければステップＳ１５３を省略することができる。

【０２１５】

コンテンツ取り込み処理：

クライアントＢ側では、クライアントＡ側でコンテンツ・データ並びにコンテンツ・コピー証明書がコピーされた記録媒体を装填して、内部に取り込むことにより、このコンテンツを利用することができる。

【０２１６】

図２０には、コンテンツのコピー先であるクライアントＢ側でコンテンツを取り込むための処理手順をフローチャートの形式で示している。

【０２１７】

クライアントＢでは、まず、装填した記録媒体からコンテンツ・データとコンテンツ・コピー証明書を取り込んで、記憶する（ステップＳ１６１）。

【０２１８】

次いで、コンテンツ・コピー証明書の電子署名を、ライセンス・サーバＢの公開鍵を用いて検証し（ステップＳ１６２）、署名が正しいかどうか、すなわちコンテンツ・コピー証明書が改竄されていないかどうかをチェックする（ステップＳ１６３）。

【０２１９】

ここで、署名が正しくない、すなわちコンテンツ・コピー証明書が改竄されていると判断された場合には、ステップＳ１６３の分岐Ｎｏからステップ Ｓ１６４に進み、所定のエラー処理を実行して本処理ルーチン全体を終了する。この場合、コンテンツ・コピー証明書からライセンスを取り出すことができないので、ク

ライアントＢ上ではコンテンツを利用することができなくなる。

【０２２０】

一方、署名が正しいと判断された場合には、次いで、コンテンツ・コピー証明書の通し番号を用いて、同一のコンテンツ・コピー証明書を既に使用したことがあるかどうかを検証し（ステップＳ１６５）、このコンテンツ・コピー証明書を用いた履歴の有無をチェックする（ステップＳ１６６）。

【０２２１】

ここで、同じコンテンツ・コピー証明書を用いた履歴がある場合には、ステップＳ１６６の分岐Ｎｏからステップ Ｓ１６７に進み、所定のエラー処理を実行して本処理ルーチン全体を終了する。この場合、コンテンツ・コピー証明書からライセンスを取り出すことができないので、クライアントＢ上ではコンテンツを利用することができなくなる。

【０２２２】

同じコンテンツ・コピー証明書を用いた履歴がない場合には、記録媒体より取り込んだコンテンツのコンテンツＩＤがコンテンツ・コピー証明書に記述されているコンテンツＩＤと一致するかどうかを検証し（ステップＳ１６８）、双方のコンテンツＩＤが一致するかどうかをチェックする（ステップＳ１６９）。

【０２２３】

ここで、双方のコンテンツＩＤが一致しない場合には、ステップＳ１６９の分岐Ｎｏからステップ Ｓ１７０に進み、所定のエラー処理を実行して本処理ルーチン全体を終了する。この場合、コンテンツ・コピー証明書からライセンスを取り出すことができないので、クライアントＢ上ではコンテンツを利用することができなくなる。

【０２２４】

双方のコンテンツＩＤが一致する場合には、コンテンツ・コピー証明書内のライセンスを取り出して、記憶する（ステップＳ１７１）。

【０２２５】

そして、コンテンツのヘッダに、取り出したライセンスのライセンスＩＤを加え（ステップＳ１７２）、これをコンテンツ蓄積部に格納する。この結果、記録

媒体から取り出されたコンテンツ・データのコピーは、図９に示したものと同じ形式となるので、コンテンツ再生処理部は通常のコンテンツ再生処理（前述並びに図１０を参照のこと）に従ってコンテンツを再生することができる。

【０２２６】

そして、最後にコンテンツ・コピー証明書の通し番号を、「使用済みコンテンツ・コピー証明書」として、クライアントＢ内に記録する（ステップＳ１７３）。

【０２２７】

なお、ステップＳ１６３，Ｓ１６６，Ｓ１６９に相当するコンテンツ・コピー証明書の正当性チェックのアルゴリズムについては、耐タンパ性のある処理として構成することが望ましい。

【０２２８】

クライアントＢでは、上述したような処理手順に従って取り込んだコンテンツ・データを図１０に示したコンテンツ再生処理に従ってコンテンツを再生することができる。

【０２２９】

まず、クライアントＢは、ユーザがキーボードやマウスなどの入力装置の操作を介して指示したコンテンツの識別情報（ＣＩＤ）を取得する（ステップＳ４１）。コンテンツが指示されると、次いで、そのコンテンツに対応するライセンスＩＤを読み取る。

【０２３０】

次いで、読み取られたライセンスＩＤに対応するライセンスが、クライアントにより既に取得され、ライセンス取得・管理部に保管されているかどうかを判断する（ステップＳ４２）。

【０２３１】

該当するライセンスが未だ取得されていない場合には、ステップＳ４３に進み、ライセンス取得処理を実行する。但し、この時点では、コンテンツ・コピー証明書から取り出されたライセンスがライセンス取得・管理部に保管されているので、ライセンスが既に取得されていると判断される。

【０２３２】

次いで、このライセンスが有効期限内かどうかを判断する（ステップＳ４４）。ライセンスの有効期限が既に満了していると判断された場合には、ステップＳ４５に進み、ライセンスの更新処理を実行する。クライアントＢは、図１４に示す処理手順に従ってライセンス更新処理を行なう。

【０２３３】

ステップＳ４４において、ライセンスが有効期限内であると判断された場合、あるいはステップＳ４５においてライセンスが更新された場合、さらにライセンスが正当であるかどうかを判断する（ステップＳ４６）。ライセンスが正当でない場合には、エラー処理を行なってから（ステップＳ４７）、

【０２３４】

ステップＳ４６において、ライセンスが正当であると判断された場合、該当する暗号化コンテンツ・データをコンテンツ蓄積部から読み出す（ステップＳ４８）。そして、暗号化されているコンテンツ・データを、図９に示したデータに配置されている暗号化ブロック単位で、コンテンツ・キーK_cを用いて復号する（ステップＳ４９）。

【０２３５】

さらに、復号されたコンテンツ・データをデコードし、コンテンツの再生処理を行なう（ステップＳ５０）。

【０２３６】

［追補］

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２３７】

【発明の効果】

以上詳記したように、本発明によれば、コンテンツの不正利用を防止しながら

、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にすることができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することができる。

【０２３８】

本発明によれば、それぞれのコンテンツ配信事業者と接続可能な別々のクライアントにて購入したコンテンツを各クライアントで共有して使用することができる。但し、別のクライアントで利用する際、それが有料又は無料のいずれであるかはコンテンツ配信事業者や著作権保有者などの独自の判断で設定することができる。

【０２３９】

また、本発明によれば、一方のクライアントで購入したコンテンツを別のクライアントと共有して利用するために課金が発生する場合には、その別のクライアントを使用するだけで課金処理を行なうことができるので、顧客の利便性が向上する。

【０２４０】

また、本発明によれば、一方のクライアントで設定又は更新した再生環境情報（再生リスト、再生設定（音量設定、連続再生設定など）、ＧＵＩ画面、購入予定楽曲へのブックマークなど）を、他方のクライアントにおいても繁栄させることができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係るコンテンツ配信システムの構成例を模式的に示した図である。

【図２】

各種サーバあるいはクライアントとして動作するホスト装置のハードウェア構成を模式的に示した図である。

【図３】

ホストがクライアントとして動作するときの機能構成を模式的に示した図であ

る。

【図４】

ホストがライセンス・サーバとして動作するときの機能構成を模式的に示した図である。

【図５】

ホストがコンテンツ・サーバとして動作するときの機能構成を模式的に示した図である。

【図６】

クライアントがライセンス・サーバに事前登録を行なうための処理手順を示したフローチャートである。

【図７】

コンテンツをダウンロードする際のクライアント側の処理手順を示したフローチャートである。

【図８】

コンテンツをダウンロードする際のコンテンツ・サーバ側の処理手順を示したフローチャートである。

【図９】

コンテンツ・サーバＡからクライアントＡにコンテンツを配信するときに用いられるデータ・フォーマットの構成例を示した図である。

【図１０】

クライアントＡ側でダウンロードしたコンテンツを再生するための処理手順を示したフローチャートである。

【図１１】

クライアントＡ側でダウンロードしたコンテンツを再生するために必要なライセンスを取得する処理手順を示したフローチャートである。

【図１２】

ライセンス・サーバからクライアントに提供されるライセンスのデータ構造を模式的に示した図である。

【図１３】

ライセンス・サーバＡがクライアントＡにライセンスを提供するための処理手順を示したフローチャートである。

【図１４】

クライアントが実行する、ライセンス・サーバに対するライセンスの更新処理の詳細な手順を示したフローチャートである。

【図１５】

ライセンス・サーバによるライセンスを更新するための詳細な処理手順を示したフローチャートである。

【図１６】

クライアントＡがライセンス・サーバＡからコンテンツ・コピー証明書を取得するための処理手順を示したフローチャートである。

【図１７】

ライセンス・サーバＡがクライアントＡからの要求に応答してコンテンツ・コピー証明書を発行するための処理手順を示したフローチャートである。

【図１８】

コンテンツ・コピー証明書のデータ構造を模式的に示した図である。

【図１９】

クライアント間でコンテンツを移動する際の、移動元となるクライアントＡ側で行なう処理手順を示したフローチャートである。

【図２０】

コンテンツのコピー先であるクライアントＢ側でコンテンツを取り込むための処理手順を示したフローチャートである。

【図２１】

クライアントが、ライセンス・サーバから供給されたライセンスに基づいて、コンテンツ・サーバから供給されたコンテンツを利用する処理の仕組みを説明するための図である。

【図２２】

ＥＫＢの構造を示した図である。

【符号の説明】

１００…ホスト

１０１…ＣＰＵ，

１０２…主メモリ，１０３…ＲＯＭ

１０４…ディスプレイ・コントローラ

１０５…入力機器インターフェース

１０６…ネットワーク・インターフェース

１０７…外部機器インターフェース

１０８…バス

１１１…ディスプレイ

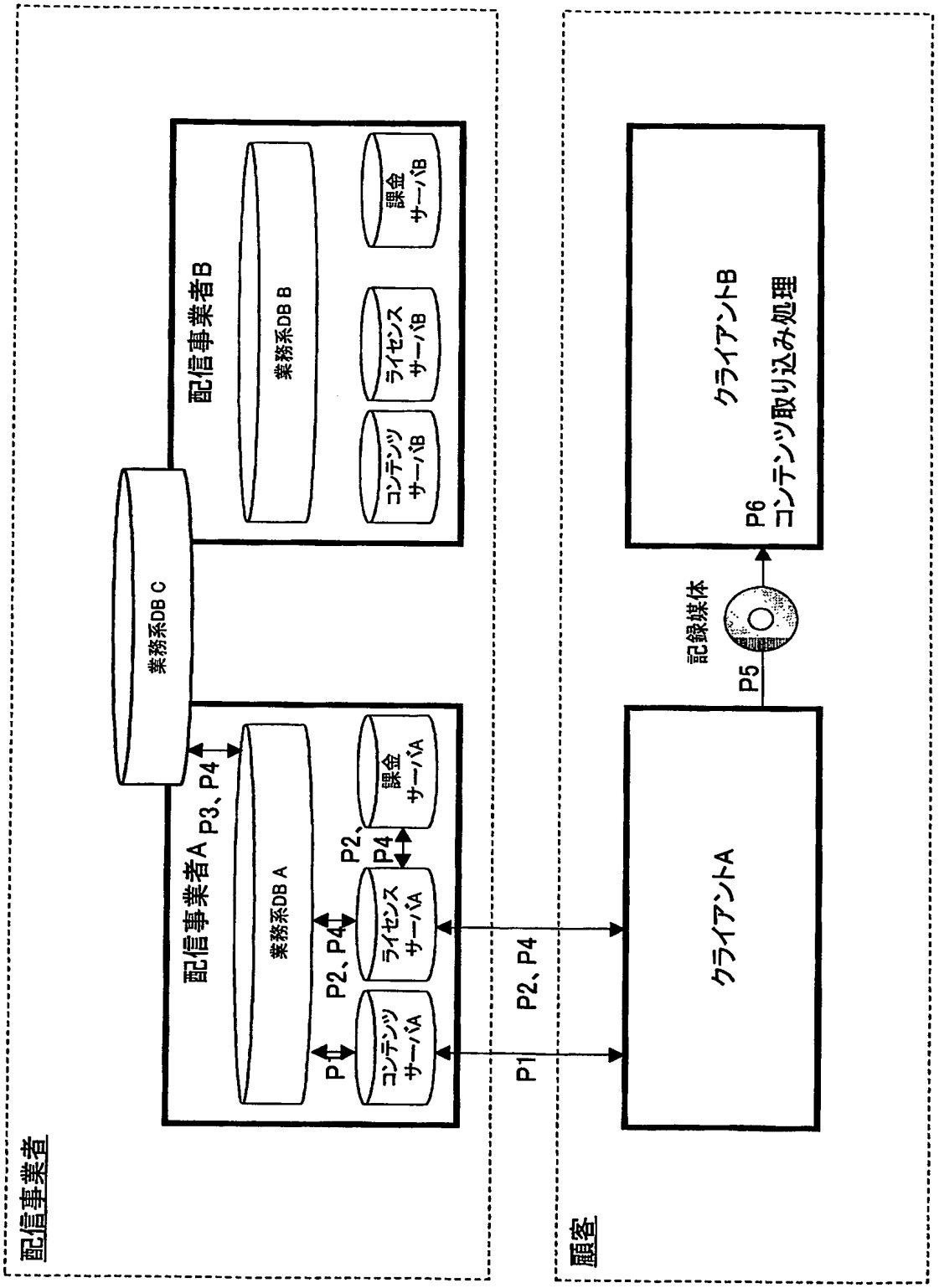
１１２…キーボード，１１３…マウス

１１４…ハード・ディスク装置

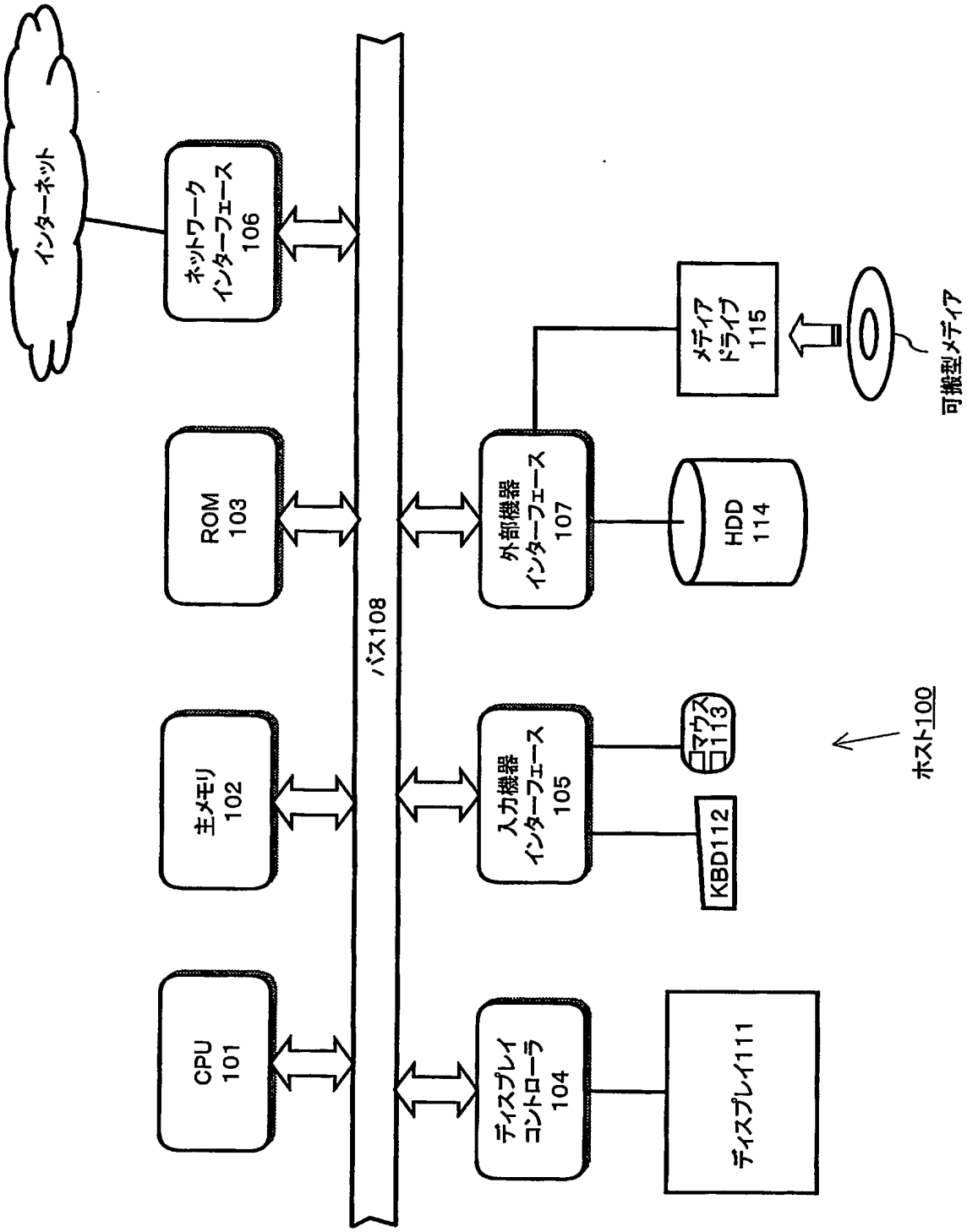
１１５…メディア・ドライブ

【書類名】　図面

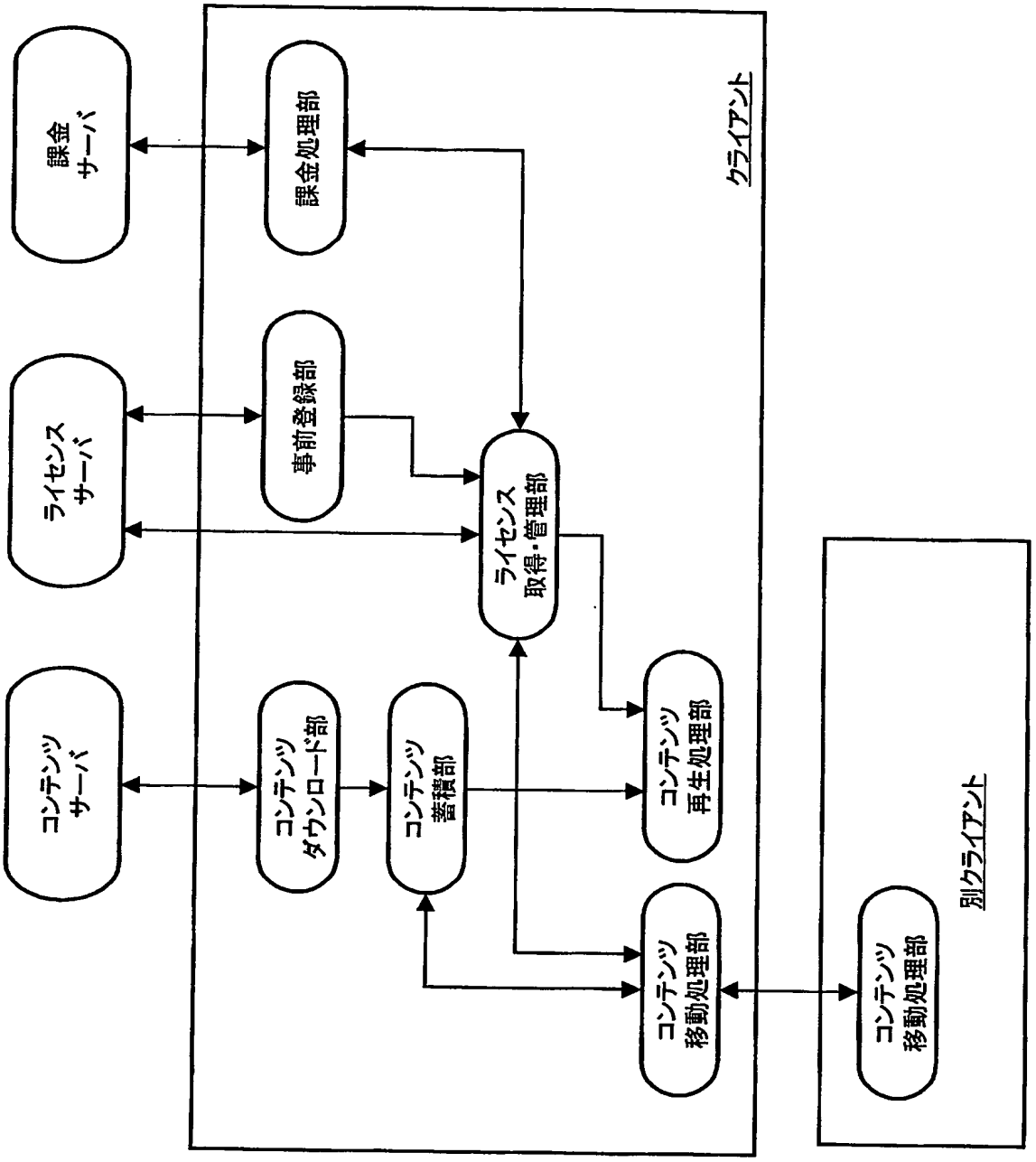
【図１】


配信事業者
顧客
配信事業者A
業務系DB A
業務系DB C
配信事業者B
業務系DB B
課金サーバA
ライセンスサーバA
コンテンツサーバA
課金サーバB
ライセンスサーバB
コンテンツサーバB
クライアントA
クライアントB
P6 コンテンツ取り込み処理
記録媒体
P5
P1
P2、P4
P3、P4

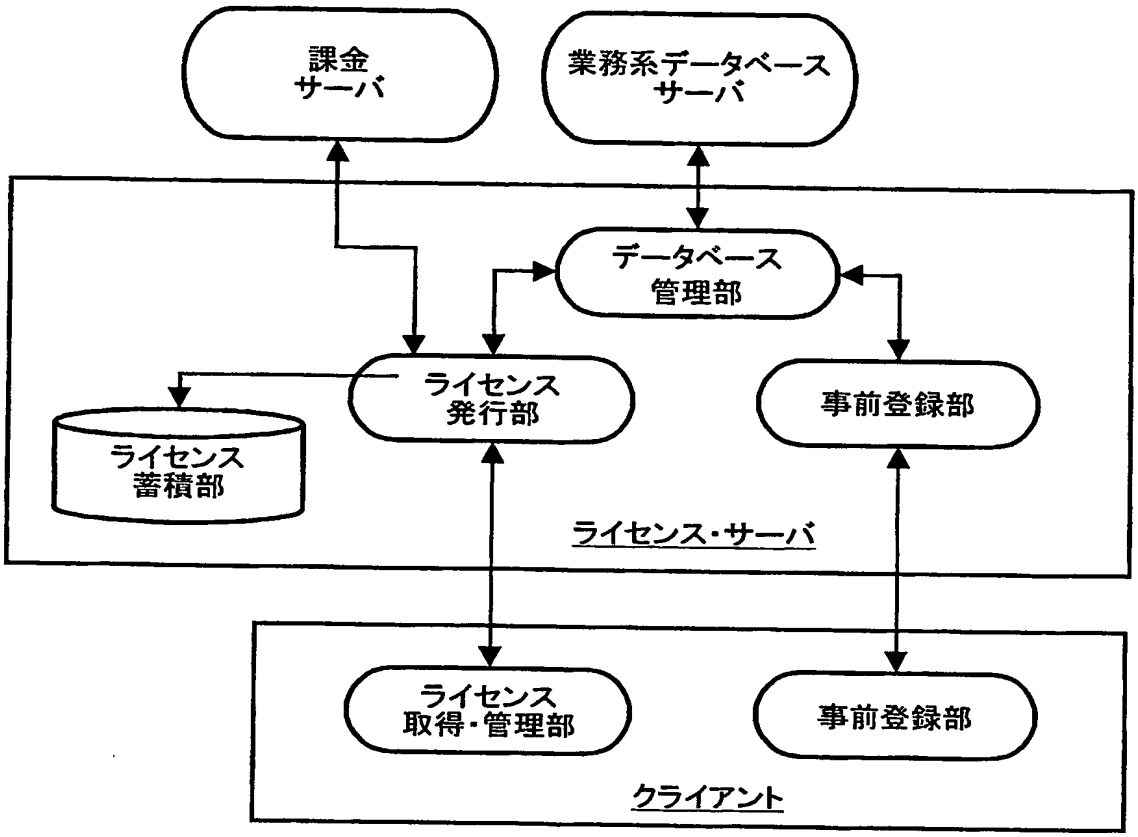
【図２】


インターネット
ネットワーク
インターフェース
106
ROM
103
主メモリ
102
CPU
101
バス108
外部機器
インターフェース
107
入力機器
インターフェース
105
ディスプレイ
コントローラ
104
メディア
ドライブ
115
HDD
114
マウス
113
KBD112
ディスプレイ111
可搬型メディア
ホスト100

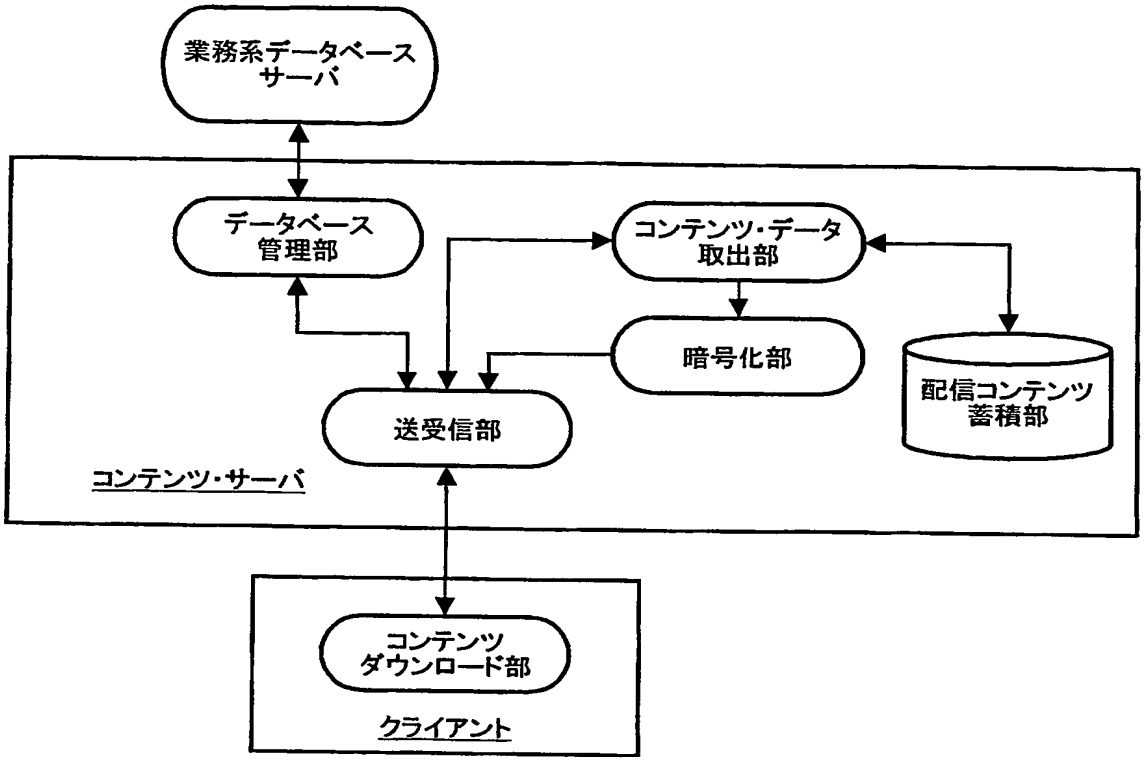
【図３】


課金サーバ
課金処理部
クライアント
ライセンスサーバ
事前登録部
ライセンス取得・管理部
コンテンツサーバ
コンテンツダウンロード部
コンテンツ蓄積部
コンテンツ再生処理部
コンテンツ移動処理部
別クライアント
コンテンツ移動処理部

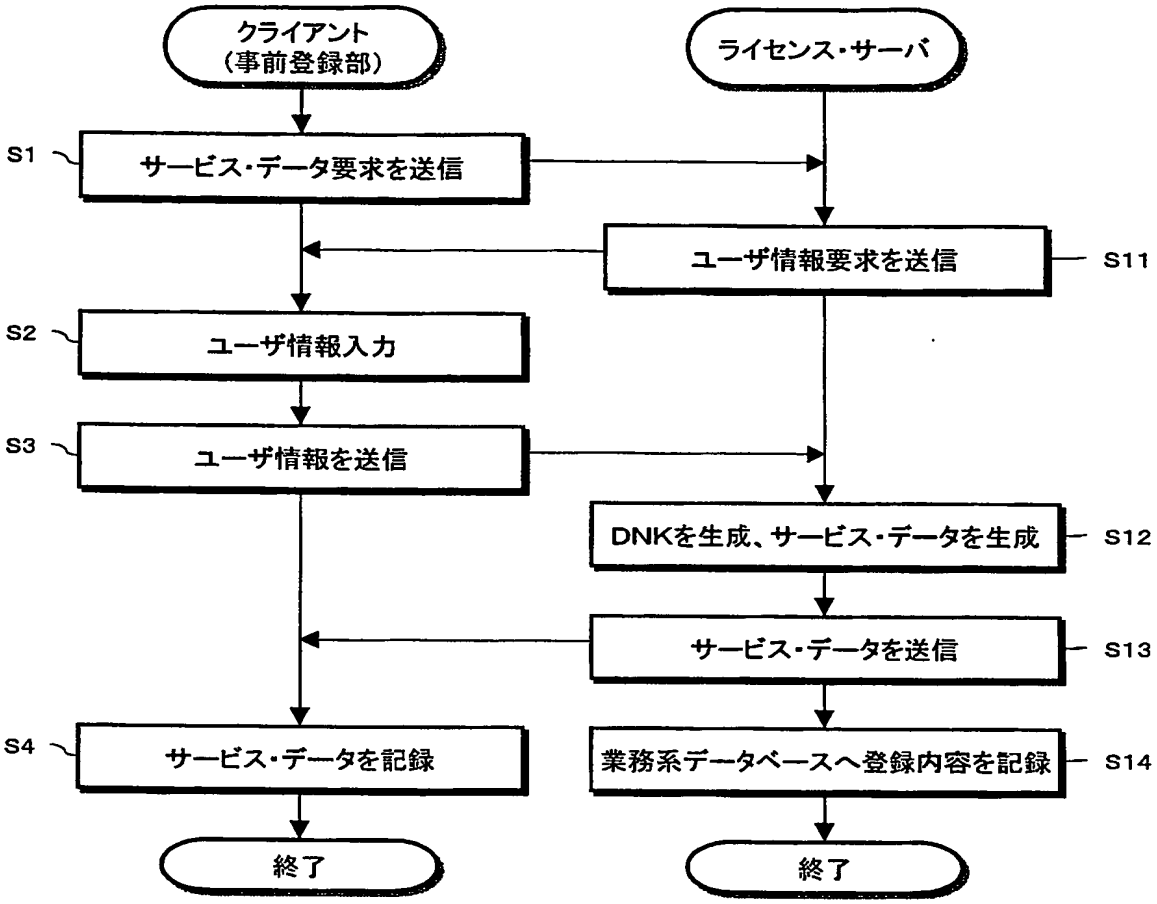
【図４】


課金
サーバ
業務系データベース
サーバ
データベース
管理部
ライセンス
発行部
事前登録部
ライセンス
蓄積部
ライセンス・サーバ
ライセンス
取得・管理部
事前登録部
クライアント

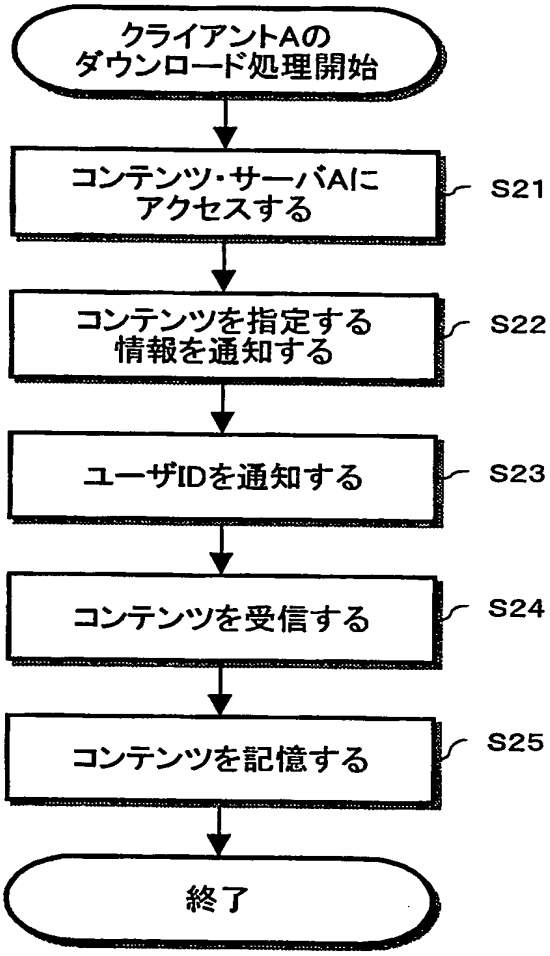
【図５】


業務系データベース
サーバ
データベース
管理部
コンテンツ・データ
取出部
暗号化部
配信コンテンツ
蓄積部
送受信部
コンテンツ・サーバ
コンテンツ
ダウンロード部
クライアント

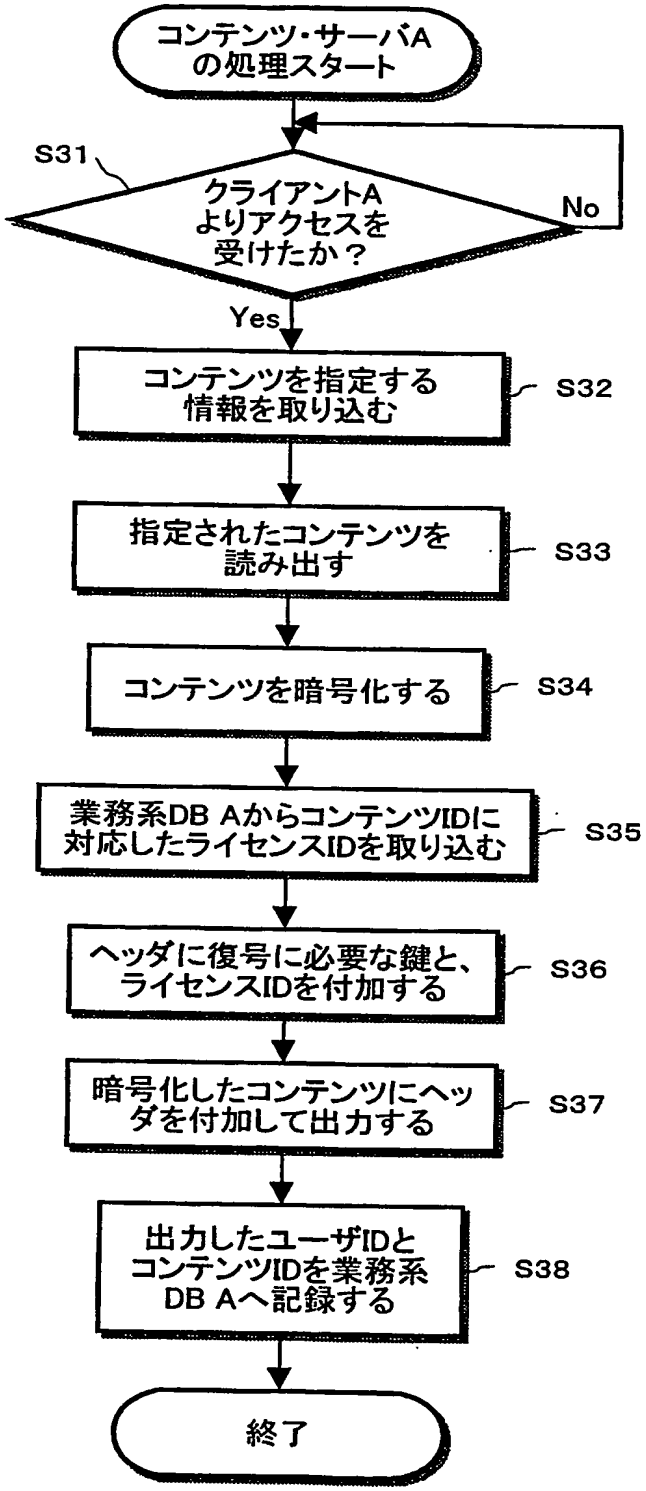
【図６】


クライアント
（事前登録部）
ライセンス・サーバ
S1
サービス・データ要求を送信
ユーザ情報要求を送信
S11
S2
ユーザ情報入力
S3
ユーザ情報を送信
DNKを生成、サービス・データを生成
S12
サービス・データを送信
S13
S4
サービス・データを記録
業務系データベースへ登録内容を記録
S14
終了
終了

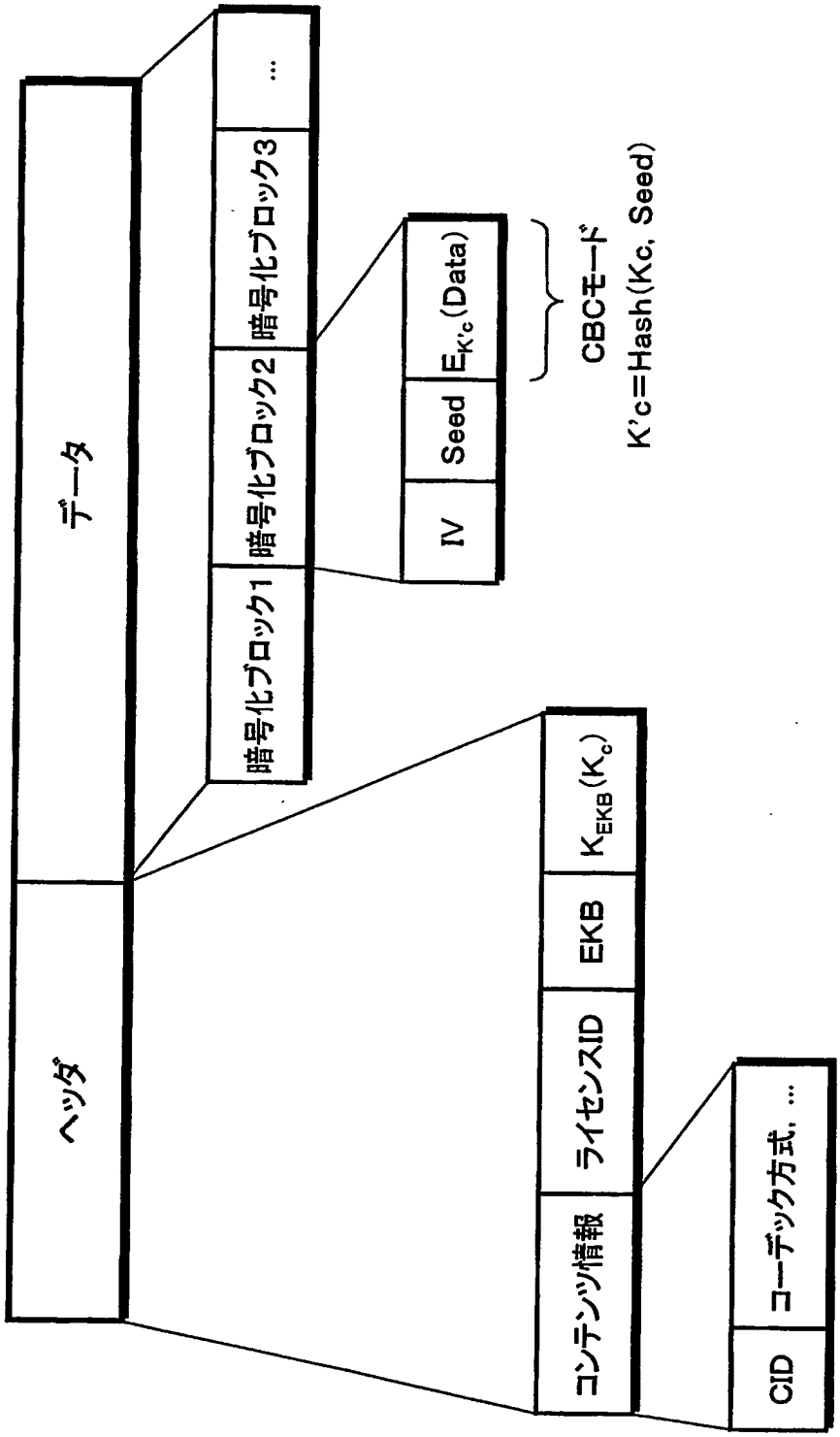
【図7】


クライアントAの
ダウンロード処理開始
コンテンツ・サーバAに
アクセスする
S21
コンテンツを指定する
情報を通知する
S22
ユーザIDを通知する
S23
コンテンツを受信する
S24
コンテンツを記憶する
S25
終了

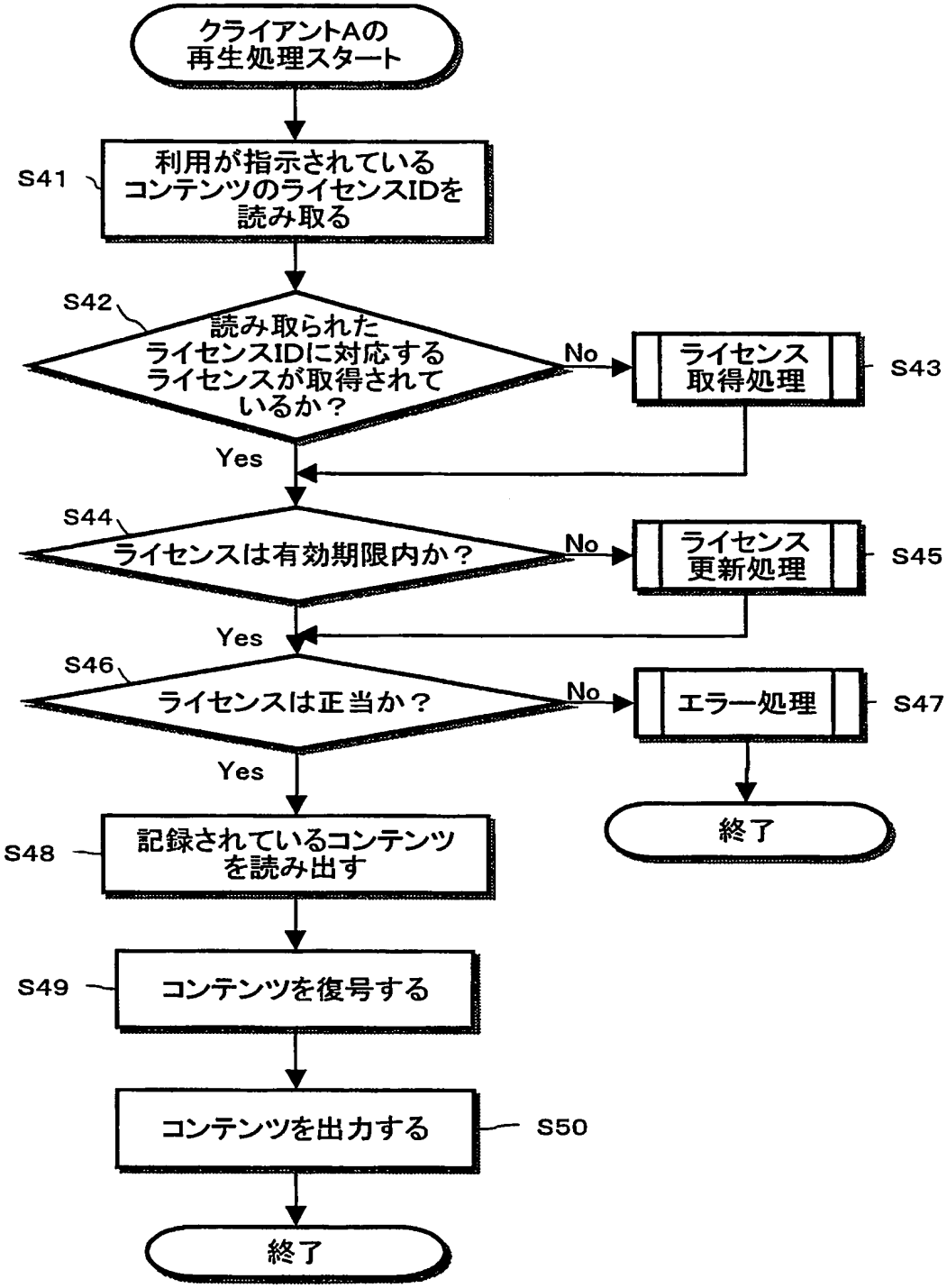
【図８】


コンテンツ・サーバA
の処理スタート
S31
クライアントA
よりアクセスを
受けたか？
No
Yes
コンテンツを指定する
情報を取り込む
S32
指定されたコンテンツを
読み出す
S33
コンテンツを暗号化する
S34
業務系DB Aからコンテンツに
対応したライセンスIDを取り込む
S35
ヘッダに復号に必要な鍵と、
ライセンスIDを付加する
S36
暗号化したコンテンツにヘッ
ダを付加して出力する
S37
出力したユーザIDと
コンテンツIDを業務系
DB Aへ記録する
S38
終了

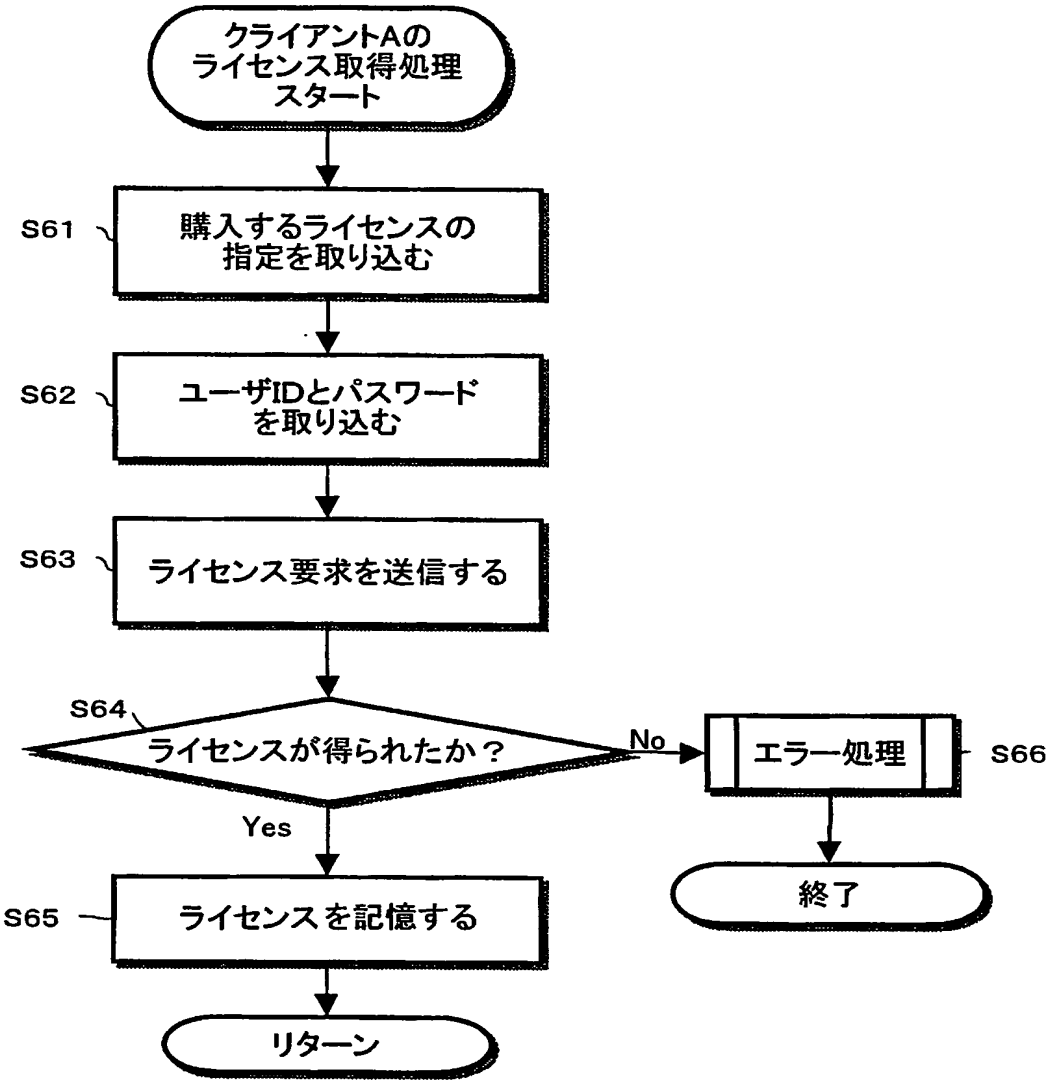
【図9】


ヘッダ
データ
暗号化ブロック1
暗号化ブロック2
暗号化ブロック3
...
IV
Seed
$E_{K'c}$(Data)
CBCモード
K'c=Hash(Kc, Seed)
コンテンツ情報
ライセンスID
EKB
K_{EKB}(K_c)
CID
コーデック方式, ...

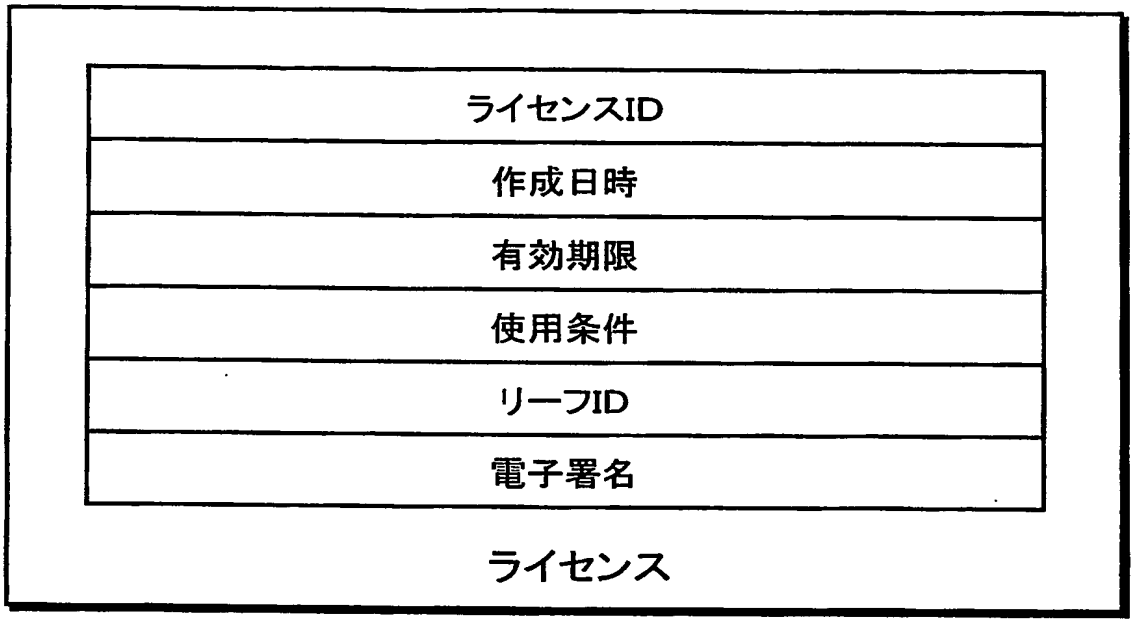
【図１０】


クライアントAの
再生処理スタート
S41
利用が指示されている
コンテンツのライセンスIDを
読み取る
S42
読み取られた
ライセンスIDに対応する
ライセンスが取得されて
いるか？
No
ライセンス
取得処理
S43
Yes
S44
ライセンスは有効期限内か？
No
ライセンス
更新処理
S45
Yes
S46
ライセンスは正当か？
No
エラー処理
S47
Yes
終了
S48
記録されているコンテンツ
を読み出す
S49
コンテンツを復号する
コンテンツを出力する
S50
終了

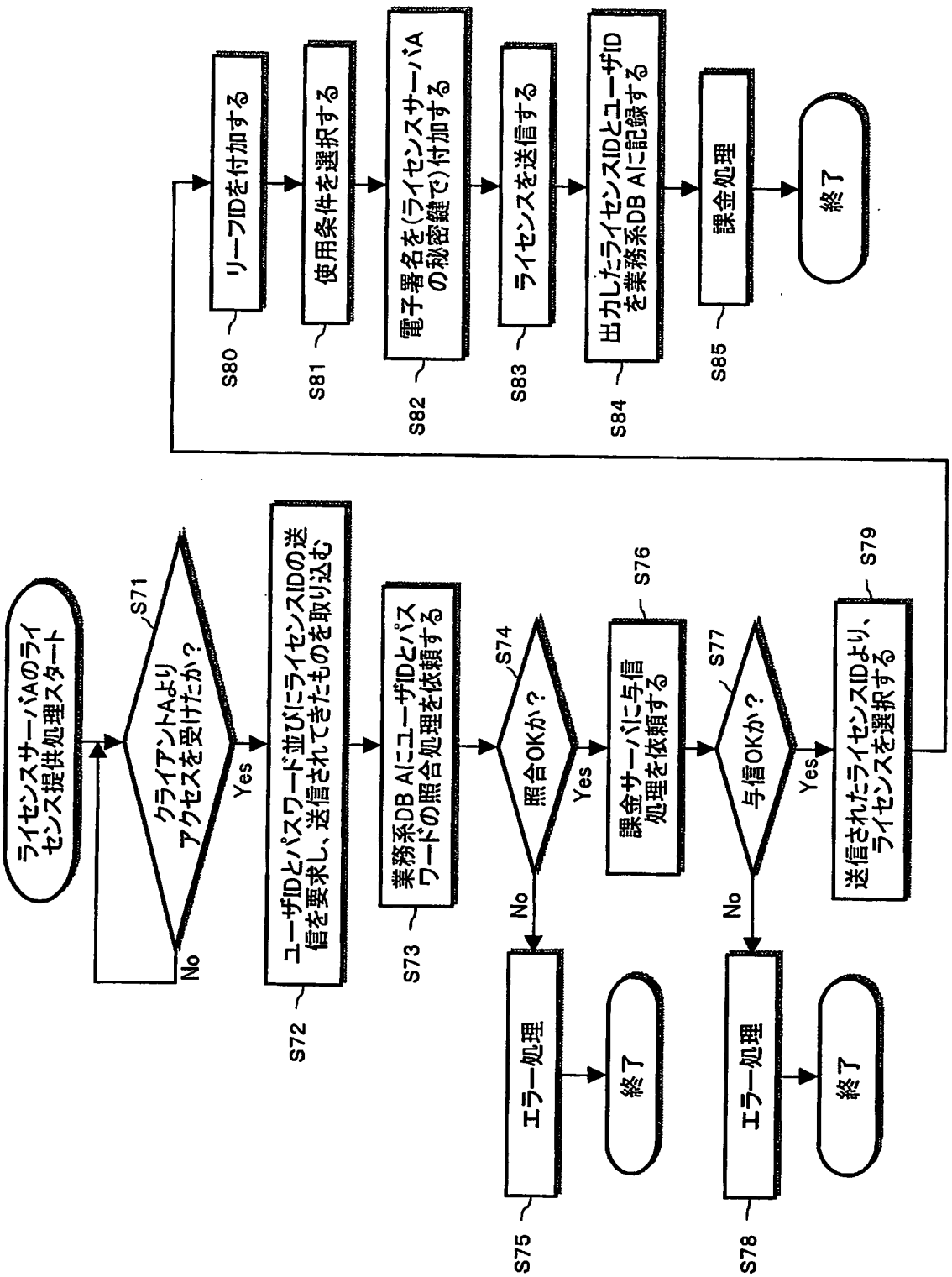
【図１１】


クライアントAの
ライセンス取得処理
スタート
S61
購入するライセンスの
指定を取り込む
S62
ユーザIDとパスワード
を取り込む
S63
ライセンス要求を送信する
S64
ライセンスが得られたか？
No
エラー処理
S66
Yes
S65
ライセンスを記憶する
リターン
終了

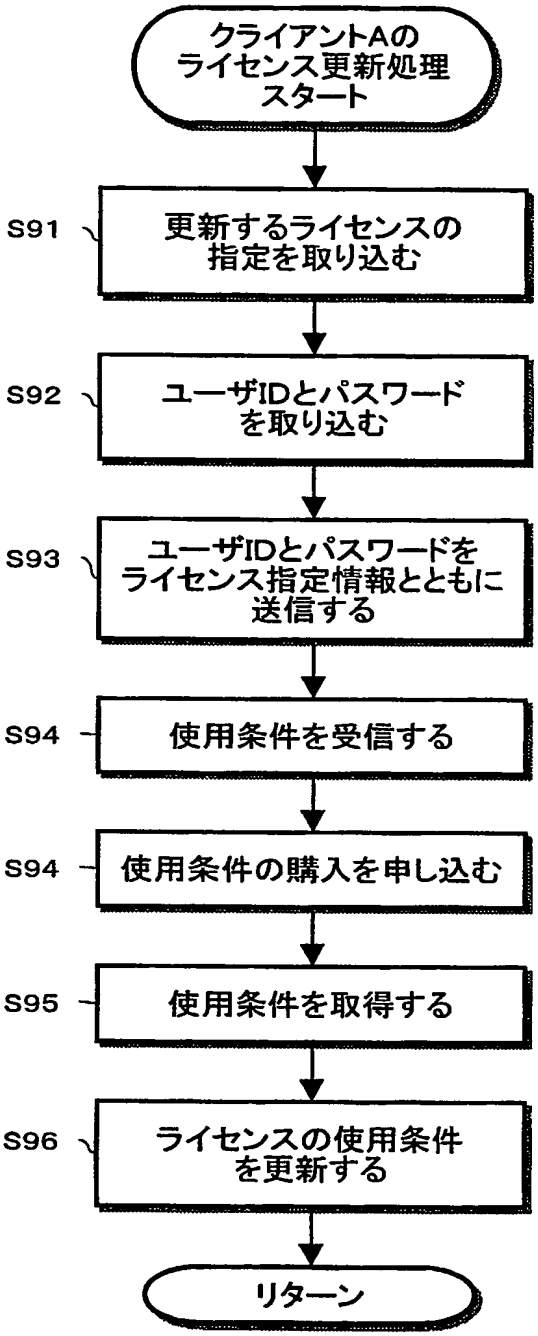
【図１２】



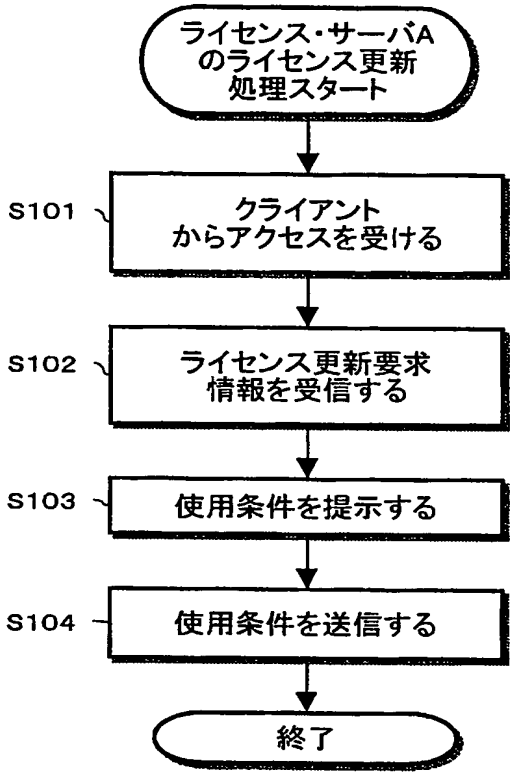
【図１３】


ライセンスサーバAのライセンス提供処理スタート
クライアントAよりアクセスを受けたか？
Yes
No
S71
ユーザIDとパスワード並びにライセンスIDの送信を要求し、送信されてきたものを取り込む
S72
業務系DB Aにユーザ IDとパスワードの照合処理を依頼する
S73
照合OKか？
Yes
No
S74
課金サーバに与信処理を依頼する
S76
与信OKか？
Yes
No
S77
送信されたライセンスIDより、ライセンスを選択する
S79
エラー処理
S75
終了
エラー処理
S78
終了
リーフIDを付加する
S80
使用条件を選択する
S81
電子署名を(ライセンスサーバAの秘密鍵で)付加する
S82
ライセンスを送信する
S83
出力したライセンスIDとユーザIDを業務系DB Aに記録する
S84
課金処理
S85
終了

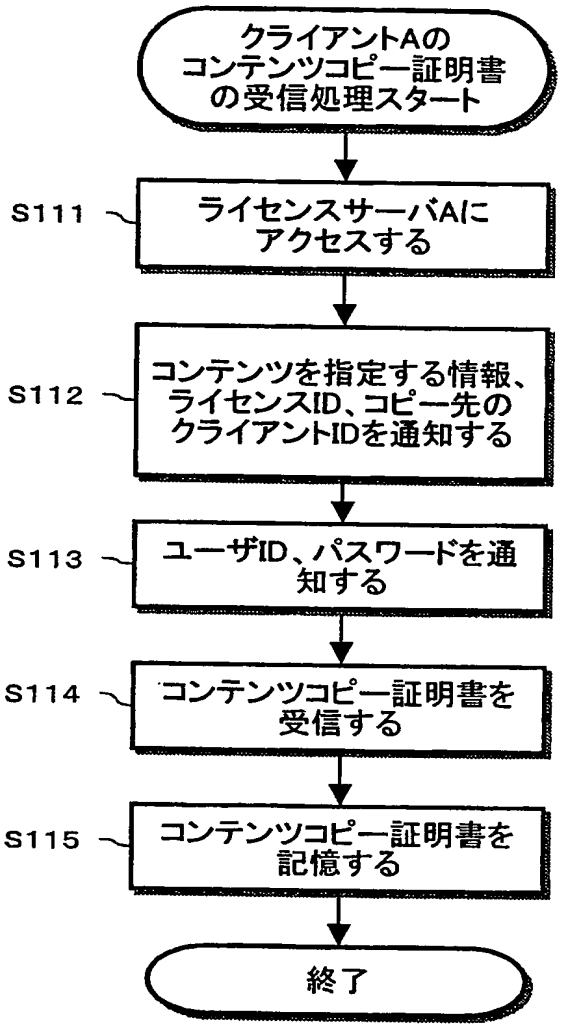
【図１４】


クライアントAの
ライセンス更新処理
スタート
S91
更新するライセンスの
指定を取り込む
S92
ユーザIDとパスワード
を取り込む
S93
ユーザIDとパスワードを
ライセンス指定情報とともに
送信する
S94
使用条件を受信する
S94
使用条件の購入を申し込む
S95
使用条件を取得する
S96
ライセンスの使用条件
を更新する
リターン

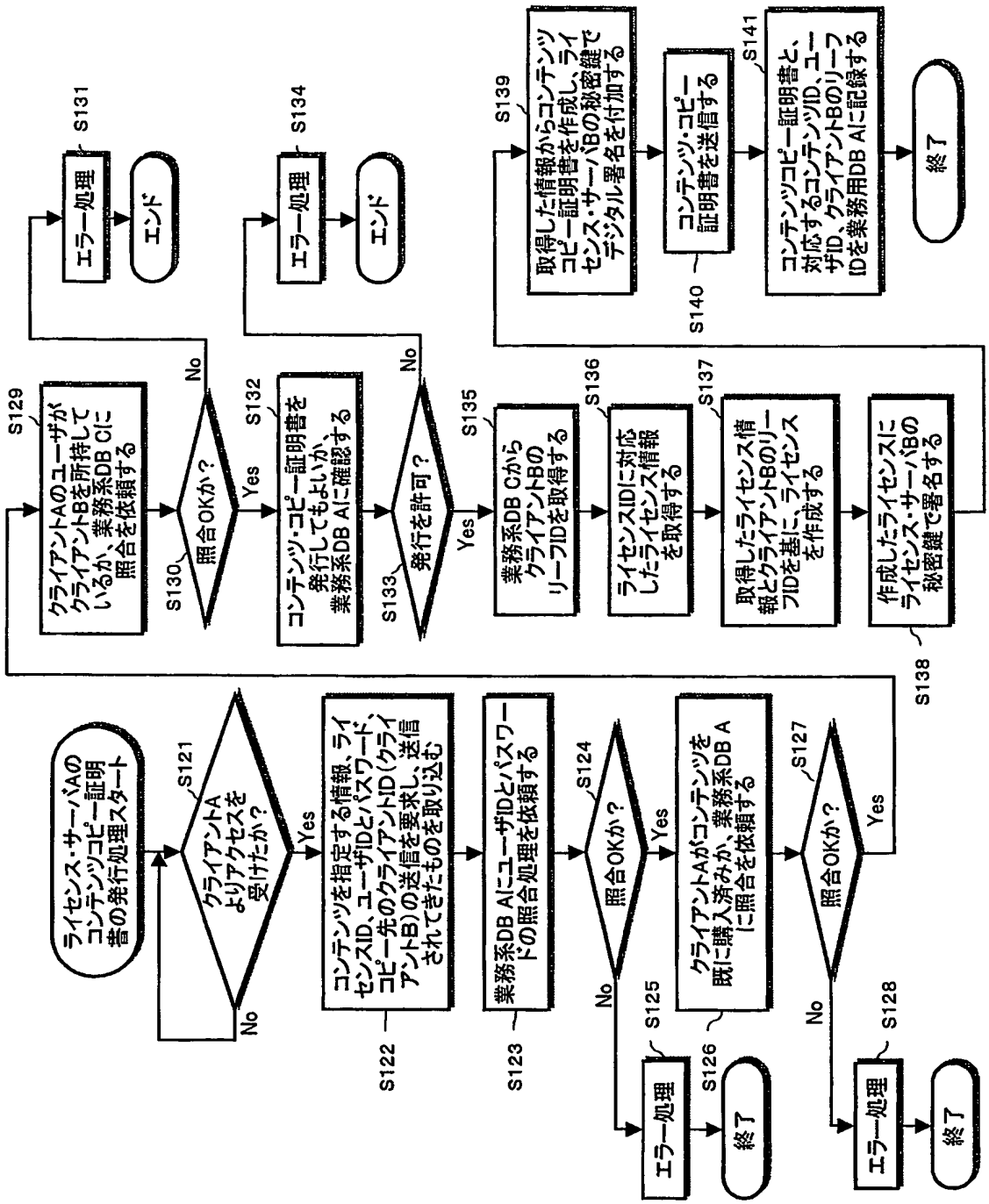
【図１５】


ライセンス・サーバA
のライセンス更新
処理スタート
S101
クライアント
からアクセスを受ける
S102
ライセンス更新要求
情報を受信する
S103
使用条件を提示する
S104
使用条件を送信する
終了

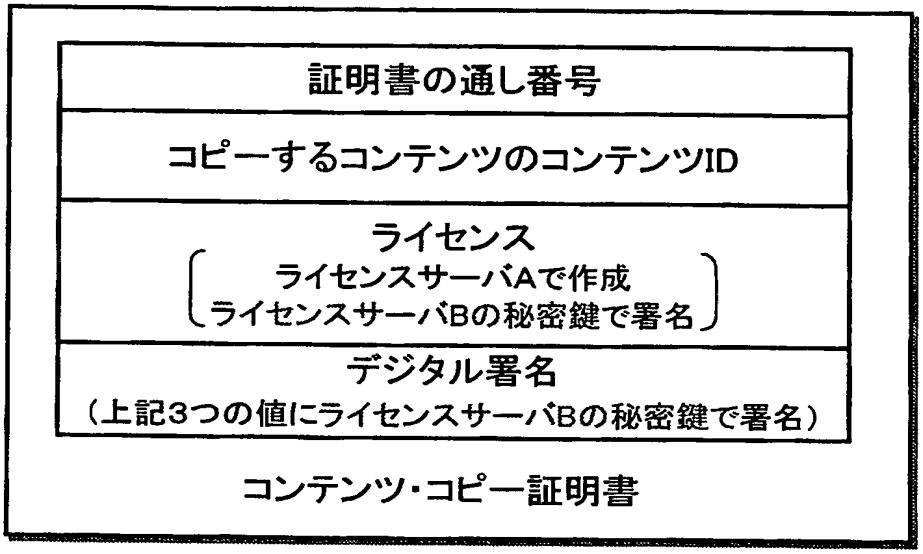
【図１６】


クライアントAの
コンテンツコピー証明書
の受信処理スタート
S111
ライセンスサーバAに
アクセスする
S112
コンテンツを指定する情報、
ライセンスID、コピー先の
クライアントIDを通知する
S113
ユーザID、パスワードを通
知する
S114
コンテンツコピー証明書を
受信する
S115
コンテンツコピー証明書を
記憶する
終了

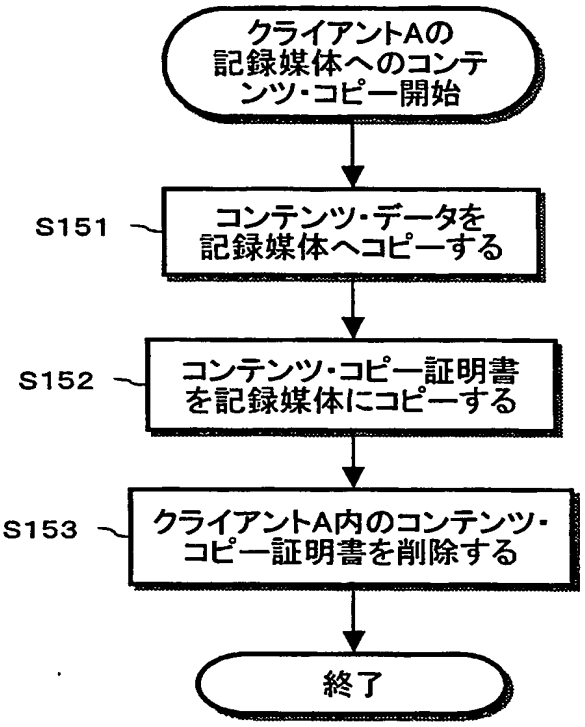
【図１７】


ライセンス・サーバAのコンテンツコピー証明書の発行処理スタート
S121
クライアントAよりアクセスを受けたか？
No
Yes
S122
コンテンツを指定する情報、ライセンスID、ユーザIDとパスワード、コピー先のクライアントID（クライアントB）の送信を要求し、送信されてきたものを取り込む
S123
業務系DB AにユーザIDとパスワードの照合処理を依頼する
S124
照合OKか？
No
Yes
S125
エラー処理
S126
終了
クライアントAがコンテンツを既に購入済みか、業務系DB Aに照合を依頼する
S127
照合OKか？
No
Yes
S128
エラー処理
終了
S129
クライアントAのユーザがクライアントBを所持しているか、業務系DB Cに照合を依頼する
S130
照合OKか？
No
Yes
S131
エラー処理
エンド
S132
コンテンツ・コピー証明書を発行してもよいか、業務系DB Aに確認する
S133
発行を許可？
No
Yes
S134
エラー処理
エンド
S135
業務系DB Cからクライアントの リーフIDを取得する
S136
ライセンスIDに対応したライセンス情報を取得する
S137
取得したライセンス情報とクライアントBのリーフIDを基に、ライセンスを作成する
S138
作成したライセンスにライセンス・サーバBの秘密鍵で署名する
S139
取得した情報からコンテンツコピー証明書を作成し、ライセンス・サーバBの秘密鍵でデジタル署名を付加する
S140
コンテンツ・コピー証明書を送信する
S141
コンテンツコピー証明書と、対応するコンテンツID、ユーザID、クライアントBのリーフIDを業務用DB Aに記録する
終了

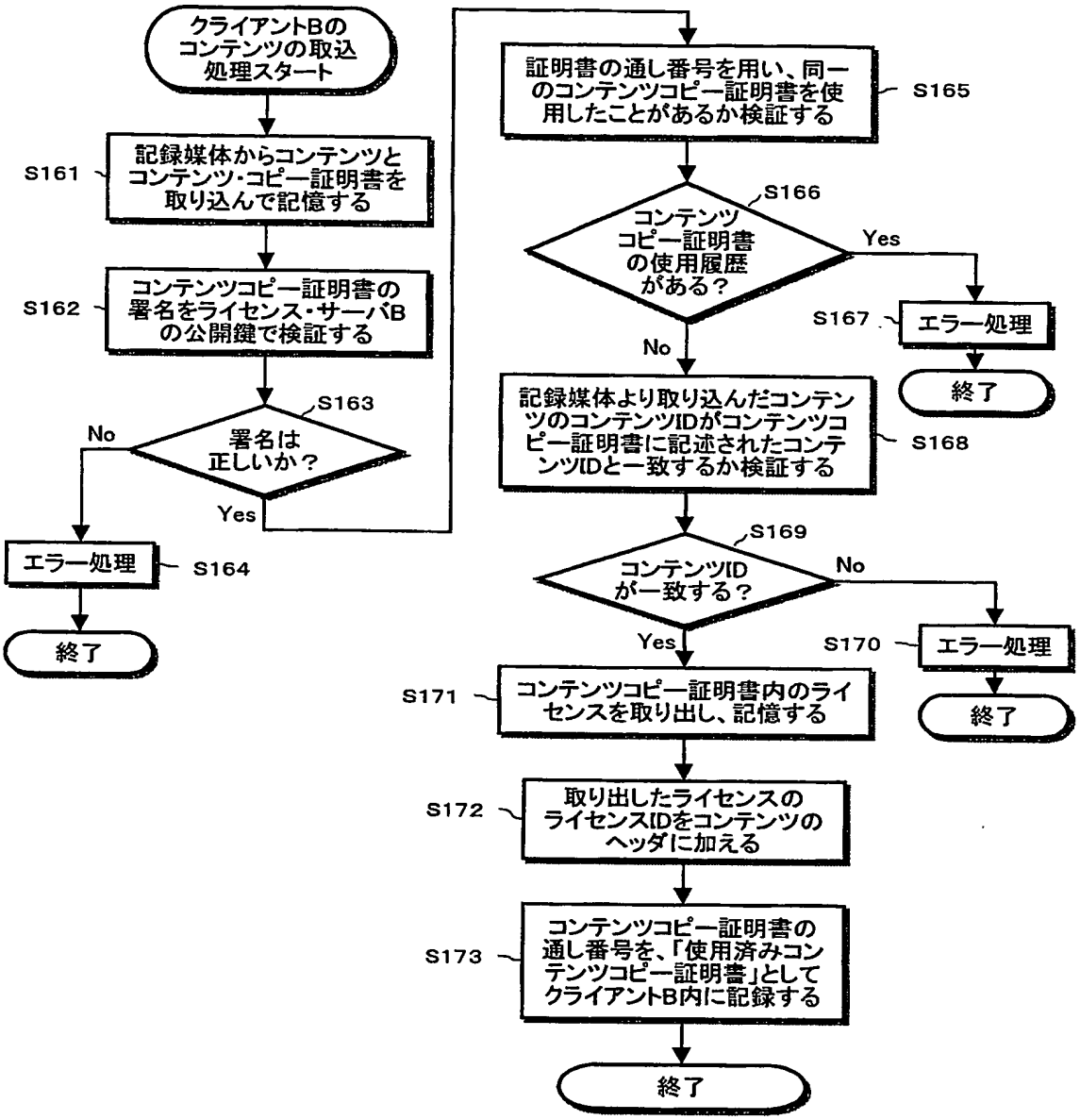
【図１８】


証明書の通し番号
コピーするコンテンツのコンテンツID
ライセンス
ライセンスサーバAで作成
ライセンスサーバBの秘密鍵で署名
デジタル署名
（上記3つの値にライセンスサーバBの秘密鍵で署名）
コンテンツ・コピー証明書

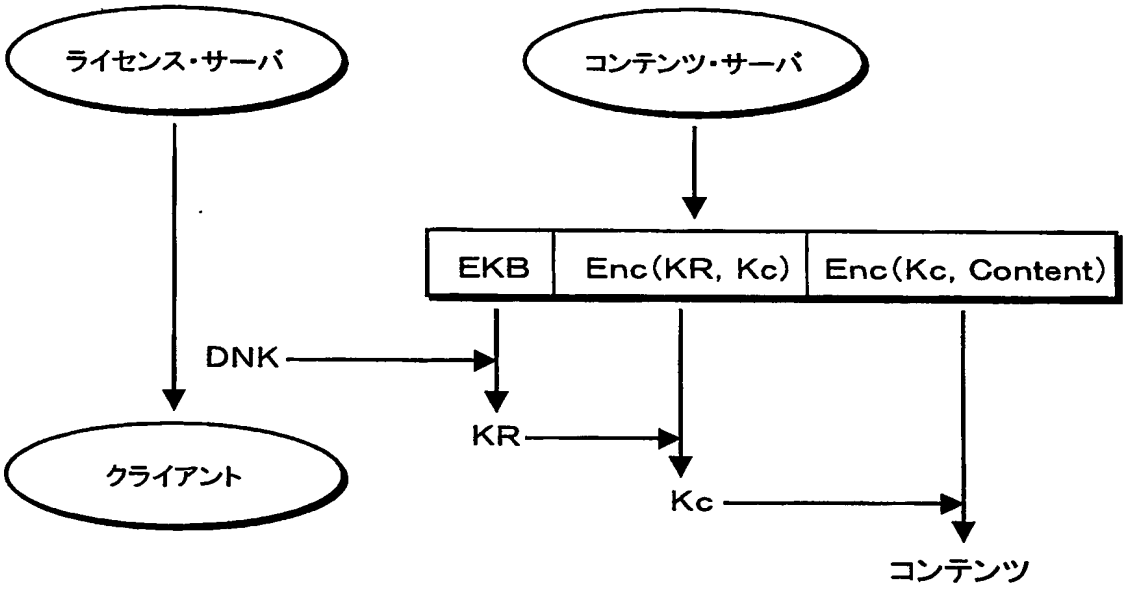
【図１９】


クライアントAの記録媒体へのコンテンツ・コピー開始
S151
コンテンツ・データを記録媒体へコピーする
S152
コンテンツ・コピー証明書を記録媒体にコピーする
S153
クライアントA内のコンテンツ・コピー証明書を削除する
終了

【図２０】


クライアントBのコンテンツの取込処理スタート
S161
記録媒体からコンテンツとコンテンツ・コピー証明書を取り込んで記憶する
S162
コンテンツコピー証明書の署名をライセンス・サーバBの公開鍵で検証する
S163
署名は正しいか？
No
Yes
S164
エラー処理
終了
S165
証明書の通し番号を用い、同一のコンテンツコピー証明書を使用したことがあるか検証する
S166
コンテンツコピー証明書の使用履歴がある？
Yes
S167
エラー処理
終了
No
S168
記録媒体より取り込んだコンテンツのコンテンツIDがコンテンツコピー証明書に記述されたコンテンツIDと一致するか検証する
S169
コンテンツIDが一致する？
No
S170
エラー処理
終了
Yes
S171
コンテンツコピー証明書内のライセンスを取り出し、記憶する
S172
取り出したライセンスのライセンスIDをコンテンツのヘッダに加える
S173
コンテンツコピー証明書の通し番号を、「使用済みコンテンツコピー証明書」としてクライアントB内に記録する
終了

【図２１】


ライセンス・サーバ
コンテンツ・サーバ
EKB
Enc(KR, Kc)
Enc(Kc, Content)
DNK
KR
Kc
クライアント
コンテンツ

【図２２】


Enc(DNK, KR)

【書類名】 要約書

【要約】

【課題】 コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にする。

【解決手段】 著作権管理されている環境が提供され、暗号化されたコンテンツと、その暗号を解くライセンスを別物で扱うことができる。また、各クライアントは正当にコンテンツを使用する。クライアントＡで取得したコンテンツをクライアントＢに保管する際に、クライアントＢの情報をそのコンテンツに付加し、クライアントＢを特定できるようにすることにより、コンテンツの保護を担保しながらクライアントＡ及びＢ間でのコンテンツの共有を実現する。

【選択図】 図１

特願２００３－０１４２４５

出　願　人　履　歴　情　報

識別番号　　[０００００２１８５]

１．変更年月日　　１９９０年　８月３０日
[変更理由]　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社